

**STATE OF FEDERAL PRIVACY AND DATA
SECURITY LAW: LAGGING BEHIND THE TIMES?**

HEARING

BEFORE THE

OVERSIGHT OF GOVERNMENT MANAGEMENT,
THE FEDERAL WORKFORCE, AND THE
DISTRICT OF COLUMBIA SUBCOMMITTEE

OF THE

COMMITTEE ON
HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

JULY 31, 2012

Available via the World Wide Web: <http://www.fdsys.gov>

Printed for the use of the Committee on Homeland Security
and Governmental Affairs



U.S. GOVERNMENT PRINTING OFFICE

76-066 PDF

WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan	SUSAN M. COLLINS, Maine
DANIEL K. AKAKA, Hawaii	TOM COBURN, Oklahoma
THOMAS R. CARPER, Delaware	SCOTT P. BROWN, Massachusetts
MARK L. PRYOR, Arkansas	JOHN MCCAIN, Arizona
MARY L. LANDRIEU, Louisiana	RON JOHNSON, Wisconsin
CLAIRE McCASKILL, Missouri	ROB PORTMAN, Ohio
JON TESTER, Montana	RAND PAUL, Kentucky
MARK BEGICH, Alaska	JERRY MORAN, Kansas

MICHAEL L. ALEXANDER, *Staff Director*

NICHOLAS A. ROSSI, *Minority Staff Director*

TRINA DRIESSNACK TYRER, *Chief Clerk*

JOYCE WARD, *Publications Clerk and GPO Detailee*

OVERSIGHT OF GOVERNMENT MANAGEMENT, THE FEDERAL
WORKFORCE, AND THE DISTRICT OF COLUMBIA SUBCOMMITTEE

DANIEL K. AKAKA, Hawaii, *Chairman*

CARL LEVIN, Michigan	RON JOHNSON, Wisconsin
MARY L. LANDRIEU, Louisiana	TOM COBURN, Oklahoma
MARK BEGICH, Alaska	JERRY MORAN, Kansas

ERIC M. TAMARKIN, *Counsel*

RACHEL R. WEAVER, *Minority Staff Director*

LAUREN CORCORAN, *Chief Clerk*

CONTENTS

Opening statement:	Page
Senator Akaka	1
Senator Johnson	3
Prepared statement:	
Senator Akaka	35
Senator Carper	37

WITNESSES

TUESDAY, JULY 31, 2012

Mary Ellen Callahan, Chief Privacy Officer, U.S. Department of Homeland Security	4
Greg Long, Executive Director, Federal Retirement Thrift Investment Board ..	6
Greg C. Wilshusen, Director, Information Security Issues, U.S. Accountability Office	8
Peter Swire, C. William O'Neill Professor of Law at Ohio State University	19
Chris Calabrese, Legislative Counsel, American Civil Liberties Union	21
Paul Rosenzweig, Visiting Fellow, Heritage Foundation	23

ALPHABETICAL LIST OF WITNESSES

Calabrese, Chris:	
Testimony	21
Prepared statement	84
Callahan, Mary Ellen:	
Testimony	4
Prepared statement	38
Long, Greg:	
Testimony	6
Prepared statement	46
Rosenzweig, Paul:	
Testimony	23
Prepared statement	99
Swire, Peter:	
Testimony	19
Prepared statement	69
Wilshusen, Greg C.:	
Testimony	8
Prepared statement	52

APPENDIX

Questions and responses for the Record from:	
Ms. Callahan	117
Mr. Long	119
Mr. Wilshusen	124
Mr. Swire	126
Mr. Calabrese	127
Mr. Rosenzweig	131

STATE OF FEDERAL PRIVACY AND DATA SECURITY LAW: LAGGING BEHIND THE TIME?

TUESDAY, JULY 31, 2012

U.S. SENATE,
SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT
MANAGEMENT, THE FEDERAL WORKFORCE,
AND THE DISTRICT OF COLUMBIA,
OF THE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:03 a.m., in Room SD-628, Dirksen Senate Office Building, Hon. Daniel K. Akaka, Chairman of the Subcommittee, presiding.

Present: Senators Akaka and Johnson.

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. I call this hearing of the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia to order.

I want to say Aloha and welcome our guests and all those who are here and interested in this hearing, and I just want to thank all of you for being here.

Today, the Subcommittee will examine the foundation for our Federal privacy and data security laws. Unfortunately, key pieces of this foundation have serious cracks that need to be fixed.

The Privacy Act, a cornerstone of Federal privacy protection, was enacted way back in 1974 to respond to the increasing ease of collecting and storing personal information in computer databases. It governs how the Federal Government gathers, shares, and protects Americans' personal information.

Despite dramatic technological change over the last four decades, much of the Privacy Act remains stuck in the 1970s. Many of the definitions in the Act are simply out of date and do not make sense in the current data environment. As a result, the Act is difficult to interpret and apply, and it provides inconsistent protection to the massive amount of personal information in the hands of the government. I want to highlight a few specific concerns.

Earlier this year, the Supreme Court restricted Privacy Act remedies. In *Federal Aviation Administration v. Cooper*, the Social Security Administration violated the Privacy Act by sharing the plaintiff's HIV status with other Federal agencies. The Court concluded that he could not be compensated for emotional distress, because Privacy Act damages are limited to economic harm. By many experts' accounts, this decision rendered the Act toothless, and

scholars across the political spectrum have called for Congress to amend the Privacy Act to fix this decision.

Additionally, agencies frequently use private sector databases for law enforcement and other purposes that affect individuals' rights. This is not covered by Federal privacy laws, which creates a loophole that allows agencies to avoid privacy requirements. We should require privacy impact assessments (PIA) on agencies' use of commercial sources of Americans' private information. This would provide basic transparency of the use of commercial databases so that individuals have appropriate protections such as access, notice, correction, and purpose limitations.

Strong Executive Branch leadership is also essential to effectively enforcing the privacy protections we do now have. Over time, Congress has statutorily required Chief Privacy Officers (CPOs) in many agencies across the Federal Government, and the Office of Management and Budget (OMB) mandated in 1999 that all agencies designate a senior privacy official to assume responsibility for privacy policy. My Privacy Officer With Enhanced Rights (POWER) Act—included in the Implementing Recommendations of the 9/11 Commission Act of 2007—strengthened the authorities of the Department of Homeland Security (DHS) Chief Privacy Officer, and I would say with positive results.

Despite OMB's mandate to oversee privacy policies government-wide, it has not named a chief privacy official since the Clinton Administration. As a result, responsibility for protecting privacy is fragmented and agencies' compliance with privacy requirements is inconsistent.

Widespread agency data breaches, and inconsistent responses when they occur, are symptoms of this problem. We all remember the massive data breach at the Department of Veterans Affairs in May 2006 where the personal information of more than 26 million veterans and active duty members of the military was exposed. After that breach, OMB issued guidance requiring agencies to strengthen safeguards for personal information and implement data breach notification policies. But implementation of the guidance has been uneven, and the number of Federal data breaches has only grown.

Recently, a contractor to the Federal Retirement Thrift Investment Board (FRTIB) was the subject of a cyber attack that compromised the personal information of over 123,000 participants in the Thrift Savings Plan (TSP). This included 43 current and former Members of Congress. I was one of them. I was concerned to learn that the Board had not followed the 2007 OMB guidance and did not have a data breach notification policy in place when they learned of the breach. I am working with the Government Accountability Office (GAO) to determine how many other agencies have not followed this guidance and determine whether there is sufficient oversight of agencies that have complied.

This builds on the substantial work GAO has completed in response to my nine previous requests on privacy and data security. I have also worked closely with GAO in drafting my Privacy Act Modernization for the Information Age Act, S. 1732, which would make the OMB guidance mandatory for agencies and fix many of the other cracks in the privacy and data security foundation.

Promoting privacy and civil liberties has been a priority during my tenure in the U.S. Senate, and I will continue focusing on this issue until the end of the year. I hope my colleagues will join me in two current efforts to address the problems raised at this hearing: S. 1732 and my amendment to the cybersecurity bill we are currently considering on the floor. Protecting Americans' privacy is a bipartisan issue that I hope my colleagues will continue to advance in the years to come.

And so, I would like to call on my brother here for any opening statement that he may have. Senator Johnson.

OPENING STATEMENT OF SENATOR JOHNSON

Senator JOHNSON. Thank you, Mr. Chairman, witnesses. I want to thank you for taking time and not only being here today but also for preparing your thoughtful testimony.

Aloha. Mr. Chairman, before I start, I am not quite sure whether we are going to have another hearing. We may, but in case we do not, I just want to say what a pleasure it has been serving with you as your Ranking Member on the Subcommittee.

I mean, you are a kind, gentle, honorable soul; and for somebody new to the Senate, this is a very nice start for me to be able to serve with someone like you. So, it has really been a pleasure. I just wanted to say that.

I want to thank you for having this hearing. I think this is very timely. The full Senate now is taking up the cybersecurity bill. One of the primary issues that we are having to deal with is the privacy aspect, and all the effects of cybersecurity, trying to maintain security within our Internet network, certainly privacy is a real consideration there. It is a serious issue. It is an important issue. It is also highly complex.

Back in February I read a book review in the *Wall Street Journal* on a book called *Abundance* by Peter Dimandis and Steven Kotler, and just to put the issue in perspective how complex this is, I just want to start reading the very beginning of this book review.

It says, "If every image made and every word written from the earliest string of civilization to the year 2003 were converted to digital information, the total would come to five exabytes."

We cannot even comprehend what an exabyte is. It is one followed by 18 zeros. So again, everything from the dawn of civilization to the year 2003, five exabytes. From the year 2003 to 2010, we were producing five exabytes of information every 2 days. Next year the authors project that we will be producing five exabytes of information every 10 minutes.

So, in the age of Facebook and Google where people are voluntarily and willingly providing all kinds of information to private companies, I think we really have to ask some very serious questions.

With technology advancing at such a rapid rate, certainly the types of questions I will be asking in this hearing are going to be pretty basic. I am new here. I was not around in 1974 when the Privacy Act was, I was around but not here, when it was enacted.

So, I am just going to be asking basic questions about what was the purpose of that, what is the purpose moving forward, how do we grapple with just this exponential growth in information and

the serious threat to our cyber networks of attack from criminals, from foreign sources, and we need to take a look at what the purpose, what the cost and benefit of governmental actions, and is there potentially a better way.

So, that will kind of be the thrust of my questions. I am really looking forward to the testimony. Again, it is very timely and, Mr. Chairman, I again want to thank you for holding the hearing.

Senator AKAKA. Thank you very much, Senator Johnson.

Now, I would like to welcome our witnesses to the hearing in the first panel. Ms. Mary Ellen Callahan, Chief Privacy Officer, at the Department of Homeland Security.

I know today is your last day at DHS. So, I want to thank you so much for your service and what you have brought to that particular office of Chief Privacy Officer, and we have so much to learn from you and your experiences that you have had thus far.

I appreciate your outstanding leadership on privacy and really wish you the best of luck in your future endeavors. Thank you so much for your service.

Mr. Greg Long, Executive Director of the Federal Retirement Thrift Investment Board, and Mr. Greg Wilshusen, Director, Information Security Issues at the U.S. Government Accountability Office.

As you know, it is the custom of the Subcommittee to swear in all witnesses. So, will you please rise and raise your right hand.

Do you solemnly swear that the testimony you are about to give this Subcommittee is the truth, the whole truth, and nothing but the truth so help you, God.

Ms. CALLAHAN. I do.

Mr. LONG. I do.

Mr. WILSHUSEN. I do.

Senator AKAKA. Thank you.

Let it be noted in the record that the witnesses answered in the affirmative.

Before we start, I want you to know that your full written statement will be made a part of the record. I would also like to remind you to please limit your oral remarks to about 5 minutes.

Ms. Callahan, will you please proceed with your statement.

TESTIMONY OF MARY ELLEN CALLAHAN,¹ CHIEF PRIVACY OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. CALLAHAN. Thank you very much, sir. Good morning, Chairman Akaka, Ranking Member Johnson.

Thank you for the opportunity to appear before you today to discuss my role as the Department of Homeland Security's Chief Privacy Officer, the Privacy Act, and the collaborative achievements of the Privacy Committee of the Federal Chief Information Officers Council.

As you know, the Department of Homeland Security is the first department in the Federal Government to have a statutorily mandated privacy officer, and for that I am eternally grateful. I have had the privilege of serving in that role since March 2009. The Homeland Security Act and the POWER Act grants the Chief Pri-

¹The prepared statement of Ms. Callahan appears in the appendix on page 38.

vacy Officer the primary responsibility for ensuring that privacy considerations and protections are comprehensively integrated into all DHS programs, policies, and procedures.

I also ensure that personal information contained in Privacy Act system of record is handled in full compliance with fair information practices. Many of my authorities are similar to those of Federal Chief Privacy Officers; but I am unique, however, in that my statutory mandate includes the authority to investigate department programs and operations.

During my tenure, I have led three major investigations of significant non-compliance with departmental privacy policy. Consistent with the office's unique position as both an adviser and an oversight body for the Department's privacy sensitive programs and systems, I recently approved the creation of a privacy oversight group within the DHS privacy office.

In addition to conducting investigations, the privacy oversight team has instituted a series of privacy compliance reviews to improve a program's ability to comply with privacy assurances.

One specific example of my office's privacy efforts is the response to the OMB guidance on safeguarding personally identifying information (PII). OMB guidance required agencies to develop and implement a policy on breach notifications which in DHS refers to as privacy incidents. In September 2007 and then updated again in early 2012, the DHS privacy office distributed its Privacy Incident Handling Guidance throughout the Department to inform employees of their responsibilities to safeguard PII. The guidance provides detailed information on how to handle all stages of privacy incidents.

To ensure that staff are cognizant of PII protections, we also recently updated our annual online training which is mandatory for all DHS employees and contractors.

One of the topics of this hearing today is the Privacy Act of 1974. The Privacy Act was passed in an era before electronic communications and databases were the norms in Federal agencies.

Nonetheless, many of the concepts embedded in the original Act are flexible enough to permit similar records to be treated consistently regardless of where they are located.

One method to address modern challenges of implementing the Privacy Act is to share best practices among Federal privacy officials. Formal council-level bodies exist for many Federal chief officers. There is no formal council-level body that exists for Chief Privacy Officers. I am, however, proud to serve as the co-chair of the privacy committee of the Chief Information Officer (CIO) Council. The privacy committee was initially formed in response to the need to coordinate on shared challenges such as information sharing and protection of personally identifiable information.

Since its formal establishment in 2009, the committee has successfully functioned as a consensus-based forum for the development of privacy policy and protections throughout the Federal Government and is thoroughly integrated into the technology initiatives occurring within the Federal CIO Council. It provides an important venue in which to share experiences, training, innovative approaches, and best practices. The committee has also led the de-

velopment of privacy standards and safeguards for emerging technologies such as cloud computing and social media.

In addition, the privacy committee this year has gathered the uniform resource locators (URLs) or the Web sites for all the privacy impact assessments and system of records notices for each of the 55 participating Federal agencies. That list of privacy impact assessments and systems of records notice are available on CIO.com. The achievements of the privacy committee indicate the vital role it serves in promoting consistent Federal privacy policy, and it has been an honor to serve as one of the committee's co-chairs.

The men and women who serve in the privacy offices throughout the Federal Government are really unsung heroes. Located in various parts of organizational structures, they strive every day to apply the spirit and the law of the Privacy Act, the E-Gov Act and related privacy laws and policies.

It has been my pleasure to serve with these colleagues as their co-chair for the last 3½ years. I want to acknowledge all the hard work that they have performed throughout my Federal service.

Going forward, I am confident the Department will continue to embed privacy protections throughout its programs and services. I am happy to answer any of your questions. Thank you, sir.

Senator AKAKA. Thank you very much, Ms. Callahan.

Mr. Long, will you please proceed with your statement.

**TESTIMONY OF GREG LONG,¹ EXECUTIVE DIRECTOR,
FEDERAL RETIREMENT THRIFT INVESTMENT BOARD**

Mr. LONG. Good morning, Chairman Akaka and Members of the Subcommittee. My name is Greg Long and I am the Executive Director of the Federal Retirement Thrift Investment Board. The five members of the Board and I serve as fiduciaries of the Thrift Saving Plan. As fiduciaries, the law directs that we act solely in the interest of the TSP participants and beneficiaries and exclusively for the purpose of providing them with benefits. Because of this fiduciary duty, Congress afforded the FRTIB significant independence. The FRTIB does not receive appropriated funds for its operations. We are funded through participant monies and our budget is not subject to review or approval by Congress or the President.

The TSP maintains individual accounts for more than 4.5 million Federal and Postal, members of the uniformed services, retirees, and spousal beneficiaries. As of June 30, the TSP held approximately \$313 billion in retirement savings.

I have been asked to discuss a number of issues, including the cyber attack that resulted in the unauthorized access of the personally identifiable information of roughly 123,000 TSP participants and payees. In July 2011, a desktop computer used by an employee of Serco, an agency contractor, was subjected to a sophisticated cyber attack. Neither Serco nor the FRTIB was aware of the attack at the time it occurred.

In April 2012, the Federal Bureau of Investigation (FBI) notified Serco that the they had discovered data that appeared to be stolen

¹The prepared statement of Mr. Long appears in the appendix on page 46.

from Serco. Serco then notified us of the cyber attack. At that time, it was unclear whether agency data had been accessed.

On April 13, we determined that personally identifiable information of TSP participants had been compromised. Within 1 hour, we notified U.S. Computer Emergency Readiness Team (U.S. CERT).

The FRTIB and Serco then worked to analyze numerous files to determine what data was accessed and which participants were affected.

On May 20, an independent verification and validation concluded that the various files that had been correctly analyzed.

On May 25, 5 days after the validated list was produced, we notified affected participants about the cyber attack. My agency sent letters to each affected participant notifying them of the cyber attack and offering them one year of free identity theft consultation, restoration, and continuous credit monitoring.

I would like to emphasize the fact that this cyber attack was made on our contractor's network. Neither the FRTIB's network nor the TSP participant Web site were affected.

As the fiduciary for a plan charged with protecting the retirement savings, data security and privacy protection are priorities for us. Over the past decade, the FRTIB has undertaken a significant number of changes to its infrastructure and established information technology (IT) technical controls to improve our IT security posture.

In addition to those information technology improvements, the FRTIB has successfully added new services for its participants. Most recently in May, we rolled out the Roth TSP option which allows for after-tax contributions to the TSP.

Many of these changes added significant complexity to the plan. The need to implement these new funds and services, in large part, mandated how we assigned our personnel and allocated funding. For example, rolling out the Roth TSP initiative was a 2-year project that required staffing from every office within the Agency.

The FRTIB has security controls in place. Completing all of the documentation and accreditation that is required in the Federal Information Security Management Act (FISMA), however, is an ongoing area of focus for our Agency.

In September 2011, I approved an Enterprise Information Security and Risk Management (EISRM) Directive. Last month, I approved policies covering 18 families of management, operational, and technical security controls.

To ensure that our privacy and data security policies are appropriate, I have commissioned a "Tiger Team" to develop a plan to improve the security posture of agency information systems.

Mr. Chairman and Members of the Subcommittee, helping people retire with dignity is what drives the employees of the FRTIB. I deeply regret the cyber attack and the concern that it has caused our participants.

I want to assure all of our participants that we will continue to pursue all new avenues to ensure the safety and security of their personal data and their retirement funds.

I would be pleased to take any questions.

Senator AKAKA. Thank you very much, Mr. Long.

Now, we will have a statement of Mr. Wilshusen. Will you please proceed.

TESTIMONY OF GREG C. WILSHUSEN,¹ DIRECTOR, INFORMATION SECURITY ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WILSHUSEN. Chairman Akaka, Ranking Member Johnson, thank you for the opportunity to testify at today's hearing on the State of Federal privacy and data security laws.

Two key laws, the Privacy Act and E-Government Act are intended to protect the privacy of Americans personal information and to specify measures that Federal agencies can take to reduce the risk of data breaches.

The increasingly sophisticated ways in which personal information is obtained and used by the Federal Government has the potential to assist in performing critical functions such as helping to detect and prevent terrorist threats and enhancing online interactions with citizens. But, they can also pose challenges in ensuring the protection of citizens privacy.

Today, I will describe the impact of recent technology developments on key laws for privacy protection and actions agencies can take to protect against and respond to data breaches involving personal information.

But, first, if I may, Mr. Chairman, I would like to recognize several colleagues of mine who were instrumental in developing my statement and who work very well in this area.

Behind me is John de Ferrari and David Plocher; and also Jeff Woodward, Lee McCracken, and Melina Asencio made significant contributions to this effort.

Senator AKAKA. Thank you.

Mr. WILSHUSEN. Mr. Chairman, technological advances since the Privacy Act became law in 1974 have radically changed the way information is organized and shared among organizations and individuals.

Federal agencies use social media services, data mining, electronic databases, and other technologies to collect, use, and maintain personally identifiable information.

These advances have rendered some of the provisions of the Privacy Act and E-Government Act inadequate to fully protect all personal information collected, used, and maintained by the Federal Government.

For example, we identified issues associated with applying privacy protections consistently to all Federal collection and use of personal information, limiting the collection and use of this information to stated purposes, and establishing effective mechanisms for informing the public about privacy protections.

Accordingly, we suggested that Congress consider amending the Privacy Act and E-Government Act to address these issues. Doing so could provide a number of benefits including: Ensuring that privacy protections are applied consistently to all Federal collection and use of personal information; providing a proper balance between allowing government agencies to collect and use such infor-

¹The prepared statement of Mr. Wilshusen appears in the appendix on page 52.

mation and limiting that collection and use to what is necessary and relevant; and providing individuals with pertinent information about what personal data are to be collected, how they are to be used, and the circumstances under which they may be shared.

Mr. Chairman, as you know, much of the personal information collected and maintained by Federal agencies is processed and stored on computerized systems and networks. Yet, these systems and networks often do not provide sufficient security safeguards to protect this information.

To assist agencies in protecting information, we have reported that they should assess the privacy implications of a planned information system or data collections prior to implementation; implement a robust information security program; and limit the collection of personal information, the time it is retained, and who has access to it.

Nevertheless, Federal systems remain vulnerable and data breaches do occur. The number of security incidents reported by Federal agencies involving personally identifiable information has risen from about 13,000 in the year 2010 to over 15,500 in 2011, an increase of 19 percent.

Thus, it is important that proper response policies and procedures be in place. Notifying individuals affected by data breaches has clear benefits such as allowing people to take steps to protect themselves from identity theft.

Such notification is consistent with agency's responsibilities to inform individuals about how their information is being accessed and used and it promotes accountability for privacy protection.

In summary, Mr. Chairman, ensuring the privacy and security of personal information collected by the Federal Government remains a challenge, particularly in light of the increasing dependence on networked computer systems that can store, process, and transfer vast amounts of data.

Updating Federal laws and guidance to reflect current practices for collecting and using personal information will be key to meeting this challenge as is the need for agencies to effectively implement data security controls and privacy protections.

Without sufficient attention to these matters, American's personal information will remain at risk.

Chairman Akaka, Ranking Member Johnson, this concludes my statement. I will be happy to answer any questions.

Senator AKAKA. Thank you very much for your statement.

Mr. Long, you testified that the Board did not have a breach notification plan in place at the time of the cyber attack because of insufficient resources.

The Board has also informed Committee staff that it does not consider itself bound by the OMB guidance because the Board is an independent entity and it decides on a case-by-case basis which OMB guidance to follow.

Please discuss your view on whether the guidance applies to the Board as well as whether you would expect any differences in the Board's approach going forward.

Mr. LONG. Senator, thank you very much.

The OMB guidance has been very useful through the data breach event and the cyber attack. We did not have a breach notification

policy in place. We review every piece of OMB guidance that comes to us, and we look at it to determine whether there is anything within that guidance that conflicts with my status and the Board status as a fiduciary. As a fiduciary, we have to act solely in the interest of the participants and beneficiaries.

In this case that guidance followed best practices. It was the right thing to do. We reviewed it and it is one of the items that we decided to get to.

However, and I regret that this happened but we did not have the breach notification policy in place at the time that the cyber attack occurred.

However, in responding to the cyber attack that guidance was followed, and it was very useful in crafting our message and determining the process that we eventually went through.

Senator AKAKA. Thank you for that.

As you know, I have offered an amendment to the cybersecurity bill we are debating on the floor to make breach notification mandatory. I think it is really critical to make certain agencies prioritize this before a breach occurs. We hope that can be done in that way.

Mr. Wilshusen, in my view, agency privacy officers have been critical to focusing attention and providing leadership on privacy issues. I advocated the first statutory CPO at DHS and I have been pleased that this position was expanded to other agencies.

There have been several proposals over the years to create a Chief Privacy Officer at OMB to manage privacy policy across the government. What do you see as the potential benefits of designating a CPO for the Federal Government as a whole?

Mr. WILSHUSEN. Well, first, I would say that it would certainly raise the profile of privacy within the Federal Government and the importance of implementing privacy protections throughout the agencies.

In addition, the position could also provide advice to others within the Executive Office (EO) of the President as well as help coordinate privacy issues across Federal agencies, even potentially helping to monitor the implementation of privacy controls and privacy protections at the Federal agencies and report on them appropriately.

Senator AKAKA. Thank you.

This question is for Ms. Callahan and Mr. Wilshusen. As you know, the recent STOCK Act requires, among other things, that the financial disclosure forms of approximately 20,000 senior Executive Branch employees be posted online, which will make them available to anyone worldwide with Internet access.

I think government transparency is critical but publishing employees' personal financial information on the Internet does raise some concerns.

So, my question to both of you is: Do you feel this is an unnecessary invasion of employee privacy?

Ms. CALLAHAN. I guess I will go first.

Thank you, Mr. Chairman. The STOCK Act has required that the financial disclosures that were required for a series of individuals, both senior status as well as political appointees, not only be available under a Freedom of Information Act (FOIA) which it al-

ways has been but to be available electronically online in a searchable fashion.

First, the privacy committee that I spoke about earlier actually has been trying to figure out some governmentwide guidance on how to address these issues and how to advise the 20 some thousand individuals whose information is impacted. We have had a lot of informal conversations with ethics councils and so on.

As a privacy advocate, I am concerned and I believe there may be some privacy considerations in two fashions. One is the potential of identity theft, and we talk about data breaches and how to protect our information and how to preserve the information.

The information that is provided on that form, even if all of the Social Securities and other sensitive information has been removed, still paints a very detailed picture of an individual that would be available for somebody to look at and to investigate.

So, not only is identity theft a possibility but theft in general could be a possibility if you notice the types of assets and the protections therein. I also worry about the chilling effect that it could have on employees or potential employees in the Federal service.

With that said, as the privacy officer with the privacy committee, we have tried to put in as many protections and give as much advice as we can in order to respond to this recent requirement.

Senator AKAKA. Thank you. Mr. Wilshusen.

Mr. WILSHUSEN. I would just say I also understand the need to balance government transparency and how government operations are conducted and by whom. But at the same time, the information that is being posted is quite personal in nature. So there are certainly privacy risks and those risks need to be balanced, as has been decided against the need for open transparency.

But GAO has not looked at this issue specifically so I cannot really comment much beyond that.

Senator AKAKA. Thank you very much and thanks for those responses.

I also want to note that a number of influential homeland security and intelligence community officials recently wrote to Congress that this requirement will create significant national security threats and could place certain Federal employees and their families in harms way.

I think it is important to look closely at these issues and make any changes that are needed to protect our national security and employee safety.

Mr. Wilshusen and Ms. Callahan, I have been disappointed that the Privacy and Civil Liberties Oversight Board (PCLOB) has been dormant for so long.

Peter Swire, who will be testifying on the second panel, has argued that the most important short-term action the Senate can take on privacy is to confirm the five nominees for the Board.

Do you agree with Mr. Swire's assessment? Mr. Wilshusen.

Mr. WILSHUSEN. I would say we have not looked at that particular issue as part of my work so I cannot comment.

Ms. CALLAHAN. As the Chief Privacy Officer at the Department of Homeland Security, the statute requires that we work with the PCLOB; and at DHS and throughout the Federal Government, the

Chief Privacy Officers are very much looking forward to working with the Board once it is confirmed.

Senator AKAKA. Thank you very much.

Senator JOHNSON, your questions.

Senator JOHNSON. Thank you, Mr. Chairman.

First of all, Ms. Callahan, I also want to thank you for your service and certainly wish you well in your next endeavor. As the co-chair of the privacy committee, let us just kind of start out. I would like to get your assessment of the range of privacy practices and controls throughout the different agencies.

Can you just kind of comment on that?

Ms. CALLAHAN. Certainly, sir. Thank you very much.

As noted in my oral testimony, there are privacy officers throughout the Federal Government. They are in different places throughout the Federal Government logistically, organizationally within the Departments.

I have been very fortunate to report directly to the Secretary thanks to the Homeland Security Act, and I think that has inured not only to my benefit but to the Department's benefit.

Federal Chief Privacy Officers are in different places reporting to different positions, whether it be the general counsel, the chief information officer, the chief financial officer; and I worry that consistency and organizational structure may lead to more inefficiencies in terms of trying to address privacy considerations.

With that said, the work of the privacy committee and the work of these individuals is really yeoman's work in that they are working every day to integrate the privacy elements. It just depends on where they are in the organizational structure they have more success or less.

Senator JOHNSON. Would you say the range in terms of uniformity of privacy standards is primarily related to what? I mean, would you say how high profile the privacy officer is in relationship to the Secretary or are there other factors at play?

Ms. CALLAHAN. I think that is a factor. I think that the culture of the agency or Department may also be a factor. There also may be a factor in the sense that if they had a privacy consideration or a problem before that may have heightened the privacy considerations.

The chairman mentioned the Veterans' Affairs Committee and the Veterans' Affairs Committee CIO is actually one of my co-chairs on the privacy committee to kind of have that nexus between technology and privacy.

Senator JOHNSON. Do you think that probably the best way of getting uniformity is really through the privacy committee then? Is that working well? Do you have any other suggestions on that?

Ms. CALLAHAN. I certainly think that has helped a lot and that has helped leverage best practices, also to leverage resources. DHS is the most well-resourced privacy office and again thank you for that.

To go and use our work to try to go across the less funded agencies, as I said, we have 55 members who are participating including, obviously, independent agencies, and I think that has been very useful.

The attention that privacy gets, including this hearing, I think will be very beneficial.

Senator JOHNSON. This might be kind of a hard question but can you name the top two or three agencies in terms of privacy compliance and maybe name two or three that really give you concern or not, probably not?

Ms. CALLAHAN. Well, the No. 1 is obviously the Department of Homeland Security. [Laughter.]

Beyond that, it probably does not behoove me even on my last day to comment.

Senator JOHNSON. Maybe privately you can give it to us.

Ms. CALLAHAN. I would be happy to, sir.

Senator JOHNSON. Mr. Long, can you give me some sense of your evaluation of how good these standards are for cyber protection, let us say, in your agency and maybe even generalize it throughout the Federal Government in comparison to the private sector?

Mr. LONG. I can comment certainly on our agency. One of the actions that we have been very busy with over the past decade has been to focus on IT improvements and architecture and technical controls.

So, we undertook a significant modernization effort in terms of hardening our server environment. We made sure that we had protection built into our new capabilities—that has been a big focus on what we do going forward.

That said, we certainly have to focus on the FISMA documentation that is required. Even with all of this, we know that there are sophisticated attackers out there. We have been a victim. Our contractor was the victim and we felt the effects of that attack.

So, we need to go back and re-double our efforts and that is exactly one of the efforts that we are going through right now. We have felt that we have focused on IT security but this is a wake-up call and we are going to look at it and look at it closely.

Senator JOHNSON. Who do you rely on in terms of advising and trying to set up your IT security?

Mr. LONG. We have internally our chief technology officer. We will focus on the chief technology person as well as the chief information security officer that reports to the head of technology.

We recently established an office that reports directly to me for enterprise risk management. In addition, we will reach out to the third-party providers of services and now we are actually reaching out to DHS to figure out whether we can learn things from different councils and then through other government bodies.

Senator JOHNSON. Are you finding DHS to be very helpful from that standpoint? I mean, is that a really good core group to go to or would you be better off going to potentially other agencies that may have, I mean, do you have a clue in terms of which agencies are hardened in terms of cybersecurity? Which ones lead the way?

Mr. LONG. In terms of our outreach to DHS prior to this event and to other agencies, it was limited. We certainly participated on the small agency counsel. We participated on multiple groups, the chief information security council.

So, we would rely on small government groups on an ad hoc basis. Now, as reaction to a cyber attack on our vendors network,

we are now trying to figure out how we can formalize that better, whether it is through DHS or other groups within the government.

And then second, in forming a team to look at these issues, to figure out whether we need to go to third-party, private institutions to assist us with remediation and best practices on technology.

Senator JOHNSON. OK. Thank you. I am almost out of time.

Are we going to do a second round?

Senator AKAKA. Yes.

Senator JOHNSON. OK. I will wait.

Senator AKAKA. Thank you very much, Senator Johnson.

Ms. Callahan, I am interested in hearing more about your experience as the only Chief Privacy Officer with the strengthened investigative authorities granted by the 9–11 Commission Act of 2007.

In my view, extending these authorities to DHS was critical, given the Department's broad homeland security authorities, but I believe these investigative powers also could provide an important check against abuses in other agencies.

So, my question has two parts. Will you please elaborate on how your work has benefited from these authorities and also discuss whether you believe they should be extended to Chief Privacy Officers across the government?

Ms. CALLAHAN. Thank you, sir.

My investigatory authority has benefited my position in the Department quite a lot. As I mentioned earlier, the investigatory authority kind of helps me have the life cycle of privacy compliance in terms of how we announce what we are going to do beforehand, how we go and have the privacy compliance reviewed to make sure that our assurances are, indeed, consistent with what we have done, and if we have had a deviation, that we have the ability to have the investigation to go and look at what went wrong and how we can help ameliorate it and mitigate it for the entire Department.

I have had three major investigations of Department noncompliance with privacy policy. In each of those, it was not just a data breach, although a data breach was involved in at least one of them.

But, it was more of a systemic circumstance where the Department as a whole could learn from it, and I will use as an example, my first investigation was actually of the Inspector General (IG) which I took a slight bit of glee about.

But what had happened was the Inspector General using financial information for their financial audits that are required, their contractor used an unencrypted Universal Serial Bus (USB) drive and passed it among each other because the DHS system was too hard to use and to utilize. So, they had it as kind of the team USB drive. That had information from the U.S. Immigration and Customs Enforcement (ICE), the United States Citizenship and Immigration Services (USCIS), the Customs and Border Protection (CBP) and other components on it because it was part of the financial concerns.

The USB drive was lost; and so, the Inspector General, consistent with his authority, did the fact-finding of what happened and kind of the facts associated therein.

I then applied a privacy analysis to the circumstances, to the noncompliance with DHS policy and also looked at avenues and ways for recommendations for the entire Department to ameliorate both the contractor use of DHS information but also when people hold other component information, what is the data breach process, what is the notification process, and the mitigation process. And, I think that was a successful example of using my investigatory authority to help further the goals of the Department.

Relatedly, I had an investigation associated with social media use which has then resulted in the management directive on the operational use of social media for the entire Department.

And, I think that those are good examples. Investigations are a significant resource drain but at the same time they really help to shape the direction of the Department, and I think that my office and the Department and its maturation in privacy policy has benefited extraordinarily from that process.

Senator AKAKA. Thank you.

Mr. Long, you testified that Serco, a contractor that assists TSP with recordkeeping was the subject of the cyber attack that we are discussing today.

How do you intend to work with current and future contractors to ensure that TSP personal information is properly secured?

Mr. LONG. Senator, thank you.

The contract in question, the one with Serco, is actually currently in the process of being designed for rebid. So, we have put out a public announcement a couple of months ago. We are in the process of designing the procurement action. We anticipate rolling that out on the street by the end of this calendar year and then awarding it the next fiscal year.

That contract, I can assure you, will have very stringent IT security restrictions built into it.

Senator AKAKA. Further, do you think Serco will continue to provide recordkeeping services for TSP in the future?

Mr. LONG. I anticipate that it will be a full and open competition. We are seeking robust competition from all parties.

Senator AKAKA. Yes.

Mr. Long, you testified that TSP has an extraordinary record retention burden. I agree that some data breaches could be prevented by limiting the time agencies retain personal information.

Will you please elaborate further on your recommendation?

Mr. LONG. Yes. One of the comments that I think you see going through the testimony is a recommendation on limiting the time that personally identifiable information is retained and that relates to one of the recommendations that we made in that currently the statute that governs what we do at FRTIB does not contain a statute of limitations for judicial review of a claim for benefits brought by a TSP participant or beneficiary.

This is an indefinite exposure to potential litigation for an unlimited period of time even after a participant takes all their accounts and is gone for years.

Therefore, we have advocated for a statute of limitations that would limit the amount of time the benefits claim is open, therefore, limiting the amount of time we would have to retain personally identifiable information. A 5-year statute of limitations is what

we recommend and that is typically longer than what is generally seen within other Employee Retirement Income Security Act (ERISA), 401(k) plan type designs.

Senator AKAKA. Thank you.

My last question. Mr. Wilshusen, you testified that the Privacy Act is ineffective in informing the public about privacy practices and policies.

For example, system of records notices published in the Federal Register often are difficult to find and to understand. Will you please elaborate on why establishing a centralized Federal Government privacy Web site as proposed in my bill, S. 1732, will help address this concern?

Mr. WILSHUSEN. Well, I think because it will provide a central location and one that is readily accessible. If it is on a Web site that users and the public can access in order to find information about the Systems of Records Notices (SORNs) or PIAs as well as other privacy protections that are available to information that is collected and used by the Federal Government that will be certainly helpful in meeting the openness principle as well as the notification of government activities for the public.

Senator AKAKA. Thank you very much. Senator Johnson.

Senator JOHNSON. Thank you, Mr. Chairman.

Mr. Wilshusen, you testified about the concept of limiting the information the Federal Government obtains and basically limiting the time that it is kept.

Can you elaborate on that point?

Mr. WILSHUSEN. Well, certainly. If Federal agencies are collecting personally identifiable information for a stated purpose, once that purpose has been achieved, if they continue to retain that information indefinitely for no other particular use, then potentially if appropriate security controls are not placed over that information, it could be subject to risk of unauthorized disclosure to someone who might be able to break into their systems or gain access to that information.

So, the principle is just for as long as you need the information, keep it, protect it. Once that need no longer exists, then get rid of it, delete it, subject to Federal records retention schedules.

Senator JOHNSON. Does any agency in the Federal Government employ that practice right now?

Mr. WILSHUSEN. I think probably in certain circumstances they might. I know, for example, that OMB had a requirement, in terms of safeguarding personally identifiable information, that if personal information is placed on agency laptop computers which are then taken out of the building and the agency determines that it no longer needs that information on those laptops, then it needs to delete it within 30 days.

To the extent that is being implemented and followed is something we have not expressly examined to date.

Senator JOHNSON. Ms. Callahan, picking up on that same point, in your privacy committee is this something that is being discussed.

Ms. CALLAHAN. In the privacy committee, we are not discussing necessarily retention periods. We are having that conversation more intra-department in terms of looking at how long we retain

information and what is the nexus between the different data retention periods and how do they impact both our mission but also the other information that is collected.

Mr. Wilshusen mentioned if there is an extract of information and put on a laptop or a USB drive, hopefully an encrypted one, we do have requirements associated with that.

But, that is just an extract of the information. The database at large, we are governed by the data retention periods. We do look at them every time the Department of Homeland Security does the statutorily required biennial review of SORNs to make sure the retention period should remain, and we do consider those issues as we renew the SORNs.

Senator JOHNSON. Are there within agencies, though, are there actually processes for deleting information?

Ms. CALLAHAN. Oh, I am sorry. There are processes for deleting information before the period, before the retention period is up.

Officials are often reticent to do that for two reasons. One because they already have an approved retention period from the National Archives and you do not want to go counter to that.

The second, there is also the question about whether or not it affects operations if you delete information on a more subjective standard as Mr. Wilshusen had argued. That is a discussion within the privacy community a lot in terms of what is the proper retention period. As I said, within the Department we have those conversations frequently.

Senator JOHNSON. You just used a word that I want to try and pick up and question you about. Counter. How many different rules, regulations, laws in the Federal Government run counter to each other when it comes to privacy?

I realize that is a really large question. But, do you have a relatively succinct answer for that or can you hit on that?

Ms. CALLAHAN. I think the tension is that the goal of the privacy officer is to support the missions and to support privacy, and retention is one element of that. I think all of the fair information practice principles are ones that you have to analyze.

And so, I think that, if you look at statutes throughout the government, the Privacy Act, 40 years old, has some elements that may be logically inconsistent with some of the other more recent statutes. Yes.

Senator JOHNSON. Let us go to the other elements that Mr. Wilshusen had talked about in terms of limiting the information. Is there any kind of robust effort, or any effort, ongoing in any agency about really taking a look at what information is really required so we do not ask for more than we really need?

Ms. CALLAHAN. I can answer that question for the Department of Homeland Security which is, yes, we are looking into ways to not collect the same information over and over from the same people if we do not have to.

One of the things that surprised me when I came to the Department was how we had a lot of the same information in 47 or however many different databases and the databases were not necessarily federated or integrated with each other. That could have privacy risks in and of itself because you have different people logging on. You may not have auditing accountability.

We are working within the Department to find an infrastructure that will allow us to be more efficient, more effective, maybe collect less information from the public, and I think that they may all cheer for that, but also to have a system that has more privacy controls and more privacy protections in terms of a way to have the databases interact.

So, we are thinking about it in the fledgling stages but that is definitely something that I think the Department is going to move forward with.

Senator JOHNSON. Mr. Wilshusen, we are debating a cybersecurity bill which, depending upon how it all turns out, might impose certain requirements, regulations on the private sector.

I just kind of want to get your feel in terms of the government's ability to meet those same types of standards. I realize that is very difficult to answer because we really do not know what those standards might be.

But can you just in general speak to the level of technical competency within most agencies, how broad that technical competency is versus the private sector?

Mr. WILSHUSEN. I would be glad to. We do quite a bit of work examining the information security controls at Federal agencies, and we look at it from different levels. One, across the Federal Government in terms of how agencies are reporting the implementation of the various different controls as part of the FISMA reporting process.

As part of GAO's responsibility to audit the government consolidated financial statements, we work with the agency's IGs to assess the effectiveness of their controls in protecting information security controls over the financial information.

Then, we do other tests of agency's information security controls as requested by Members of Congress. We have been reporting that Federal information security has been a high risk area, a governmentwide high risk area since 1997.

Just most recently, the work that we have done and in reviewing the work also of the IGs, the majority of the 24 major CFO Act agencies have weaknesses in most of the information security controls that we review.

And, these would include access controls or those controls are designed to restrict, limit, and detect unauthorized access to resources as well as other security management programs and their procedures for managing the configurations of their devices.

By and large most of those agencies have weaknesses in those areas.

Senator JOHNSON. Just one quick followup.

Can you access or make an evaluation in terms of the competency between the Federal Government and those agencies in the private sector? Because you are going to see the weaknesses in the private sector as well.

Mr. WILSHUSEN. In the few instances where we have examined the security controls at private sector organizations that are performing services for the Federal Government, we have found the same types of security weaknesses in those systems as we do in the Federal systems.

Senator JOHNSON. OK. Thank you very much.

Senator AKAKA. Thank you very much, Senator Johnson.

I want to thank our first panel very much for your responses, your statements, and your valuable offering here. I would like to wish you well in your work and hope we can continue to work together on privacy and security issues as well.

So, thank you very much for being here.

I would ask that our second panel come forward. I want to welcome our second panel.

Mr. Peter Swire, C. William O'Neill Professor of Law at Ohio State University. Mr. Swire had a previous engagement in Seattle, Washington, he will be testifying by teleconference this morning.

Mr. Chris Calabrese, Legislative Counsel at the American Civil Liberties Union (ACLU). And, Mr. Paul Rosenzweig, who is a visiting fellow at the Heritage Foundation. Thank you all so much for being here.

As you know, it is the custom of this Subcommittee to swear in all witnesses. So, will you please rise and raise your right hand.

Do you swear that the testimony you are about to give this Subcommittee is the truth, the whole truth, and nothing but the truth so help you, God?

Mr. SWIRE. I do.

Mr. CALABRESE. I do.

Mr. ROSENZWEIG. I do.

Senator AKAKA. Thank you very much all of you.

Let it be noted for the record that the witnesses have answered in the affirmative.

Before we start, I want to remind you that your full written statements will be a part of the record. We ask you to please limit your oral remarks to 5 minutes.

Mr. Swire, please proceed with your statement.

**TESTIMONY OF PETER SWIRE,¹ C. WILLIAM O'NEILL
PROFESSOR OF LAW AT OHIO STATE UNIVERSITY**

Mr. SWIRE. Mr. Chairman, and Ranking Member Johnson, thank you for asking me to testify here today for this hearing on Federal privacy, and thank you also letting me testify remotely. I was unable to be in Washington today.

I would like to congratulate Mary Ellen Callahan for her service at DHS and the leadership she has shown to the Federal agency privacy community over time.

In this testimony, there are a lot of issues we could talk about. I am going to briefly talk about four issues.

Chairman Akaka, as you said, I think that the Senate should promptly confirm the five nominees for the Federal Privacy and Civil Liberties Oversight Board. This is the most important short-term action the Senate can take on privacy.

With the cybersecurity legislation, we are going to have potentially a lot more information sharing and the PCLOB is the way to have the oversight to go with that. All five nominees for the PCLOB have been voted out of the Judiciary Committee and all

¹The prepared statement of Mr. Swire appears in the appendix on page 69.

five have been supported by the 9/11 commission cochairs, Kean and Hamilton.

There were some dissenting votes in the Committee for the proposed chairman, David Medine. He is an outstanding nominee. He was a senior civil servant at the Federal Trade Commission (FTC) on privacy for many years. He has done work at the law firm of WilmerHale with compliance. He really has a workable realistic sense of things.

It is important to confirm the chairman as a part of the slate because only the chairman can hire staff by statute. So, unless we confirm the full slate, we will not have an oversight Board.

The second topic I am going to discuss is the idea of having a Federal Chief Privacy Officer. Senator Akaka in S. 1732 would create this by statute.

I had a role similar to that when I was chief counselor for privacy in the Office of Management and Budget under President Clinton and that has not been repeated as a position.

I think such a position has three advantages. It can coordinate across agencies, and new issues come up all the time as we were hearing. Here is one example. Drones is an issue that hits the Federal Aviation Administration (FAA) but up until now drones have not had to deal with privacy; but if they come through out the U.S. airspace, we have new privacy issues and we should have a sort of coordinated Federal response to the privacy issues there.

Second, a Federal Chief Privacy Officer could help with clearance across agencies so we have coordinated policy. And third, increasingly there are international issues, transborder issues for privacy, and so having that work correctly overseas is, I think, very important.

In doing this, I think it helps to have a statute. We have seen the DHS have the outstanding agency privacy activities in large part because your Committee put that into the statute and has supported the position that Mary Allen Callahan has been in. And I think that without a statute, it is easy for OMB not to move forward and really create the office.

My testimony suggests that the Chief Privacy Officer might take the lead on nonclassified information systems whereas the PCLOB perhaps would take the lead on oversight for classified information systems.

So, the third point I would like to get to is some loopholes in the Privacy Act as written. And, the proposed S. 1732 correctly recognizes there is a loophole in the Privacy Act for the definition of system of records.

The current definition applies only to records that are retrieved by name; but with modern search engines, we often retrieve things in lots of other ways and then turned up the names.

So, the proposed amendment would close the loophole and it would have the effect of requiring a much greater number of system of record notices for Federal agencies.

In my view having more of these SORNs, would create compliance burdens for agencies but not necessarily give us the biggest pay off in terms of privacy.

So, my testimony suggests a more promising approach might be to improve the privacy impact assessments under the E-Gov Act.

For instance, we could post these PIAs to a unified Web site. We could have public comments on the PIAs, and agencies could be required to respond to these public comments and I think this might be a more effective way to put attention on the most important privacy related systems.

The fourth in my four points is that the oversight process for this Committee could focus more attention on the line between what is identified and de-identified data in Federal agencies.

De-identification is a way where we can get uses from the data. We can look for patterns and all of that but still have privacy protection. Recently, the Federal Trade Commission has proposed a promising approach for de-identifying data for the private sector.

I think we can learn from that initiative, and also I will be working with the future privacy forum this year on a project on how to do de-identified data better.

So, in conclusion, I thank the Committee for the service of drawing attention back to these issues of Federal agency privacy policies and I look forward to trying to help with any questions. Thank you.

Senator AKAKA. Thank you very much, Mr. Swire.

Mr. Calabrese, would you please proceed with your statement.

TESTIMONY OF CHRISTOPHER R. CALABRESE,¹ LEGISLATIVE COUNSEL, AMERICAN CIVIL LIBERTIES UNION

Mr. CALABRESE. Good afternoon, Chairman Akaka, Ranking Member Johnson. Thank you for the opportunity to testify on behalf of the American Civil Liberties Union on the Privacy Act, a landmark statute that now requires a major update from Congress.

The Privacy Act lays out citizens rights and Federal agency responsibilities for the handling of personal information. The Act controls when records can be collected and how they can be disclosed, provides notice and mandates agencies keep secure, accurate, and accessible records.

But, the Act has always had some major loopholes and has become even more outdated over time. Agencies often sidestep access, accuracy, and relevance requirements by taking the many permissible exceptions under the Privacy Act. They also avoid the Privacy Act's prohibitions on disclosure by labeling any and all sharing as routine.

Additionally, the Act only protects systems of records when an agency retrieves information about a specific individual or information tied to that individual. Hence, it does not apply to techniques such as data mining which use pattern-based searches not tied to an individual.

Finally, the Federal Government often uses commercial databases which frequently contain incorrect information and are outside the protections of the Privacy Act.

Major steps toward fixing these problems can be found in Senator Akaka's legislation.

As we have heard, agency notice when personal information is lost or stalled in is a serious and ongoing problem. The ACLU believes that existing OMB guidance is inadequate. It gives far too

¹The prepared statement of Mr. Calabrese appears in the appendix on page 84.

much discretion to individual agencies as to whether to disclose these embarrassing breaches.

The Supreme Court has also weakened the remedies under the Act. In a case called *FAA v. Cooper*, decided in March, the court held that when an agency disclosed an individual's HIV status, he could not recover damages for mental or emotional distress the matter how severe because he did not suffer financial harm as a result of the violation.

This decision is particularly harmful because the damage from privacy disclosures is often an embarrassment, anxiety, and emotional distress, precisely what the court forecloses.

Finally, despite improvements from some agencies, oversight remains inadequate. This reality is as we have heard troubled times already embodied by the PCLOB, which is tasked with monitoring agency information sharing practices related to terrorism.

As we have heard, it existed in its current form since 2007 but a full slate of nominees was not put forward by either President Bush or President Obama until late last year and the Board is still vacant.

Significant misuse of personal information has resulted from these erosions of Federal privacy protections. The most recent example of this trend is the sweeping changes the National Counterterrorism Center (NCTC), made to its guidelines on the collection and use of information about U.S. persons not suspected of wrongdoing.

Previously, NCTC discarded information on U.S. persons not connected to terrorism within 180 days. However, under its new guidelines, NCTC keeps this information for up to 5 years.

This collection may be happening as a so-called routine use under the Privacy Act. This change, along with others affecting how NCTC analyzes and shares information, now allows the agency to perform searches on people with no connection to terrorism and shares the results for a wide variety of purposes with almost anyone.

By fully exploiting loopholes in the Privacy Act, NCTC can turn the vast power of the U.S. intelligence community on innocent Americans. Using personal information for different purposes, and sharing it broadly are precisely the type of harm the Privacy Act was enacted to prevent.

The Federal Government collects an enormous amount of personal information so people can receive benefits and services, exercise fundamental rights like voting or petitioning the government, getting licenses for everything from purchasing a handgun to businesses and industry, for employment, education, and for many types of health care.

This information collection is nearly ubiquitous in American life. None of this would have been a surprise in 1974. According to the congressional findings from the Privacy Act, the use of information technology can greatly magnify the harm to the individual; and so, in order to protect privacy, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

Congress must once again take up that duty and protect personal information on all of us by updating the Privacy Act. Thank you.

Senator AKAKA. Thank you very much Mr. Calabrese for your statements.

Mr. Rosenzweig, please proceed with your statement.

**TESTIMONY OF PAUL ROSENZWEIG,¹ VISITING FELLOW,
HERITAGE FOUNDATION**

Mr. ROSENZWEIG. Thank you very much, Mr. Chairman, Senator Johnson. I appreciate the opportunity to be with you today.

I take a very different perspective, I think, on the Privacy Act. I think I share the view of almost everybody who has spoken that the Privacy Act is outdated. Any act that was passed at a time when the personal computer did not exist cannot hope to match the current technological structures we have.

Where I think I differ is in thinking that we can fiddle around at the edges with modifications and extensions of older conceptions. To my mind, the technological revolution is so great that it is really time for a wholesale reconceptualization of what the Privacy Act is and how we deal with privacy.

We stand at the cusp of a technological revolution, indeed, not at the cusp but in the midst of it. We are not just doing exabytes but yottabyte and zettabytes of data every day, all of it in unstructured formats, but that is being matched by massive increases both in processing capacity and data storage capacity that allow people to make sense of this data in new and different ways.

The new sense making that we are doing is of great value. It is of value commercially to people who want to sell things; but as relevant to this Committee, it is of value to the government. It is of value to the government in counterterrorism and in law enforcement.

It brings with it acknowledgedly the threat that it may also be put to purposes which we would not want the government to do, things like targeting people because of their political beliefs or something like that but we can no longer maintain the artificial categories of use distinctions, purpose distinctions, data retention rules that are being destroyed essentially by the technological changes that are happening around us.

We retained data in the NCTC for an increased amount of time not because we want to target America's political beliefs but because we have come to learn that we cannot predict today how much value there will be in this information 5 years from now and what particular pieces of information will be of value to, say, a new terrorist investigation.

We have seen in counterterrorism investigations, at least when I was in the Department 5 years ago, data searches that go back 8, 10, 12 years. This is the type of reality that we must deal with while at the same time recognizing that there is the threat of misuse.

To my mind, the best way to ensure the privacy of citizens in America today, the reasonable privacy of citizens, is to no longer tie our conceptions to older technological constructs of word searches by name or by date.

¹The prepared statement of Mr. Rosenzweig appears in the appendix on page 99.

Rather, we should focus instead on use and purpose limitations that are inconsistent with those current capabilities and the threat environment.

We should better focus the privacy rules on what I think are, and I will admit this, much more difficult questions of defining what is and is not an appropriate consequence that can be imposed from the use of data, that is, structuring when we can take that data and impose an adverse consequence on an American citizen.

That requires a much finer degree of analysis at the back end rather than categorical imperatives at the front end: use only for this purpose, keep only for this long, when you cannot, in any way, define those in advance with any degree of clarity.

To my mind, while many of the improvements that are proposed for the Privacy Act will certainly work marginal increases in the benefits that we would gain to privacy in the system, in the end they are going to be overtaken by technology and we will wind up, if we do not take this task on, with a government use of data analytics and a privacy rule that restricts us to a locked-in technology that is where we are today while both the commercial sector in America, and more important from my perspective, our peer competitors outside of the United States rush ahead with technological advancements that we have denied ourselves because of fears of technology.

That does not suggest that we cannot ignore the possibility of misuse. Indeed, as my testimony suggests, I think that enhanced oversight and audit are the key ways to go forward in doing that; but categorical rules are, in my judgment, a straight jacket and should be eschewed.

With that, I look forward to answering your questions. Thank you.

Senator AKAKA. Thank you very much for your statement, Mr. Rosenzweig.

Mr. Swire, you testified forcefully about OMB's leadership void in Federal privacy policy and the need for a Federal Chief Privacy Officer to spearhead the interagency clearance process and represent the Administration on international privacy matters.

Why, in your view, has OMB not taken on a stronger leadership role in privacy and what steps should OMB be taking?

Mr. SWIRE. So, Senator, I would say that one thing I did see when I was in OMB is that the headcount in the Executive Office of the President is closely guarded. There is a very strict limit on how many people can be employed within OMB.

And so, when they are making choices about working on the Federal budget and doing all of the management tasks that they are doing, they are very cautious about adding staff.

At the peak of my time there, I had myself, two full-time people, and a detailee, and that was with a lot of work to get up to the staff at that level.

I think what we see, and this is what happened with Howard Schmidt in the cybersecurity czar position is that there needs to be a way where OMB and the Executive Office of the President work with the agencies to provide more staffing.

That is just a lot of work to set up and I really do think that having a pretty good nudge from Congress will help put that in

place; and without it, it just seems like a large challenge that is hard for them to put together bureaucratically.

Senator AKAKA. Thank you.

Mr. Calabrese, you testified that the Privacy Act does not extend to the Federal Government's use of commercial databases. Some of these databases may have a high level of inaccuracies. Even though their use may affect Americans' rights, there is no notice about their use and no process for individuals to correct their records.

Will you please elaborate on this problem and how we could achieve better transparency of the Federal Government's use of commercial databases?

Mr. CALABRESE. Thank you, Senator Akaka.

Well, of course, the first answer is we could adopt your amendment as part of the cybersecurity bill. It has in it a provision that says that commercial databases will be required to comply with the E-Government Act which is, of course, a close companion to the Privacy Act which requires agencies to disclose how they are using databases, where the information comes from, the sources of it, and that is a very important transparency tool.

Right now, we really do not have a feel even for how agencies are accessing these records, where they are coming from, what they are relying on. Many of these databases started as marketing databases.

So, if you were compiling a database to sell magazine subscriptions, 80 percent accuracy or 90 percent accuracy was great. If you got a few wrong, it was just a few wrong subscriptions. Obviously, that same standard cannot apply when agencies are performing vital functions.

So, I think we start with the transparency provision. We learn where this information is coming from, what they are using with it, then we can begin to figure out how it should be properly regulated.

Senator AKAKA. Thank you, Mr. Calabrese.

Mr. Rosenzweig, the Supreme Court's ruling in *FAA v. Cooper* earlier this year restricted Privacy Act remedies; and by many experts' accounts, rendered the Act, as I mentioned, in my statement, toothless.

Experts including Jim Harper at Cato have urged Congress to amend the Privacy Act so it is clear that individuals are compensated for proven mental and emotional distress.

Do you agree that we should amend the Privacy Act to restore these remedies?

Mr. ROSENZWEIG. Senator, I think that the much superior way of ensuring Federal compliance with the Privacy Act is through the mechanisms that we established, the privacy officers in the various communities, the oversight of Inspectors General of this Committee.

Those deal much more effectively, in my judgment, with systematic errors. The oversight you had today of the thrift board is a perfectly good example.

To my mind, in general, the private litigation system is a less efficient and effective way of creating systematic change. That is not to say that I disagree that most of the privacy harm is psychic in nature because most of privacy is about our own senses of personal

value, shame, whatever it is that you are protecting rather than economic harm.

But at the same time, I think that enhancing litigation over individual Privacy Act violations would actually be a diversion of resources from a much more effective and systematic way of addressing the real privacy failures that do happen in the government that should be addressed through privacy officers, Inspectors General, the PCLOB if it ever gets started, this Committee, that sort of thing.

Senator AKAKA. Thank you.

After that answer, let me ask Mr. Swire and Mr. Calabrese whether you can reflect on this or what do you think about this? Mr. Swire.

Mr. SWIRE. On the Privacy Act damages question, I would support putting back in place the way I thought the law was before. I think that the interpretation by the courts was more narrow than was intended by the Privacy Act. I think emotional harms that are proven to a jury, or to a judge are real harms here and we should put that back in the law.

Senator AKAKA. Thank you.

Mr. CALABRESE. And I would simply note that I do not think this is a diversion of resources but a supplement of resources. We already have oversight by Federal agencies and I agree that is appropriately systematic and necessary; but individuals are still harmed by these disclosures, and the harm goes far beyond the economic arm.

As such, it should be recognized. Individuals should be compensated. The Federal agencies and the Federal Government is requiring this information. So, hence, it is also required to protect the people and that information when it is lost or misused.

Senator AKAKA. Thank you very much. Senator Johnson, your questions.

Senator JOHNSON. Thank you, Mr. Chairman.

Let me start with the more philosophical question. Since 1974, or quite honestly even prior to that, versus 2012 has the definition or maybe I should state it, has the expectation of privacy changed?

I will start with you, Mr. Rosenzweig.

Mr. ROSENZWEIG. I think it changes all the time. I think that we live in a society now in which people go on Jerry Springer and meet their ex-wife's new boyfriend and have a fight with him on public TV.

I think that the expectation changes with catastrophic events. We have a different expectation of what is an acceptable privacy intrusion at airports today than we did before. Many people do not like that but the expectation is changing nonetheless.

I think that what we are really talking about in many contexts is kind of not privacy so much as an expectation of anonymity or lack of governmental scrutiny without justification, and that too seems to be changing.

But, by that, I mean that we are now in a time where people have come to understand that so much of their life is out there on Facebook, on twitter voluntarily or involuntarily because the credit card systems have changed.

But, where we are right now is that people expect that the gaze of law enforcement, for example, will not turn on them without a good justification or reason. That is a pretty different change from what it used to be which was that we expected that we were totally obscure and that the government did not even know anything about us. Now, we think that it knows about us; we just do not want it to pay attention.

Senator JOHNSON. Mr. Calabrese, do you want to add to that or challenge it?

Mr. CALABRESE. Yes, I would actually disagree candidly. I think that while people have different interpretations of privacy, I think the values that underlie privacy are really the bedrock of this country.

I mean, they start with a Fourth Amendment. They start, essentially, with the right to be left alone. People interpret that in different ways.

I think younger people, when I talk to them, believe very strongly in privacy. They interpret it a little differently. They think of it more as information control. I decide who sees what about me rather than the anonymity that we talked about in previous generations.

But, I think, this bedrock principle that I should be free from government scrutiny certainly and government interference in my private life is one that is a fundamental thread in American values.

Senator JOHNSON. Mr. Swire.

Mr. SWIRE. I have a right not to go on Jerry Springer and a right not to have Federal agencies gather all the data that Jerry Springer might get out of some of his interviews.

The enduring values goes back to the Fourth Amendment saying that there should be no unreasonable searches and seizures. What is reasonable changes with the facts.

But, I think a book by Alan Westin from around 1970 called *Privacy and Freedom* goes through the history over time and shows that the values that are at stake are very enduring. Technology changes somewhat, the safeguards change somewhat but the link between privacy and freedom is a very long-standing one.

Senator JOHNSON. Thank you. I think most people recognize the harm of loss of privacy when it comes to theft of either assets or certainly identity, certainly the harm caused by disclosure of health circumstances, that kind of stuff, can you also speak on other types of harm caused by loss of privacy and exposure of private information? Personal and private information.

Mr. Calabrese, we will start with you.

Mr. CALABRESE. Yes, no, of course.

It is such a wide variety. I think we can begin with the harm of surveillance. I fear to learn about particular things, visit particular Web sites because it may muzzle me. I may not want to visit a Web site that talks about radical Islam in spite of the fact I am the furthest thing from a radical Islamic.

I fear that will somehow be connected with me and I will suffer some investigation or harm because of it.

Then, more general just dignity reasons. I mean there are plenty of things that we do in our life that we would not want taken out

of context, whether it is just the songs we listen to or the people we are friends with.

All of these things are sort of the right to a personal life. That is really the fundamental piece here is that it is very difficult to explore new ideas, to learn about new concepts and to just sort of engage in the thought process that is necessary to be a responsible citizen in a democracy without the privacy to make mistakes, to explore ideas that you may want to later discard, all of that really requires privacy. And if you do not have it, it is sort of a fundamental harm to your right as a citizen.

Senator JOHNSON. Mr. Rosenzweig.

Mr. ROSENZWEIG. I agree that privacy is an enabler of personal development. And so, it strikes me that is the value that we want to protect, but it is just an enabler.

What we want to protect is the ability to develop personally, to speak freely as you will. The problem or the challenge that we face right now is we might want to protect the ability to develop personally through privacy protections, they are going away. Right?

If you engage in any sort of activity on the web today, it is out there. We can limit what the government does with it but there is no way that we can limit anything beyond the pieces of the government that we control, that you control.

We can maybe limit commercial sectors here in the United States. We cannot limit what happens in Bermuda. We cannot limit what happens in Mexico.

The challenge, I think, right now is to enable that personal development not by having to self-edit because of the fear of going to a Muslim Web site but by being much more strict about prohibiting adverse consequences on people for going to look at radical Islamic Web sites.

So, I do not disagree with the end result. My problem is that the way of doing it by deliberately making the government or the commercial sector dumb about what people are doing is the wrong way to go about it.

The right way to go about it is let us be smart but then make us do smart things with the smart data, not stupid things like challenging people just because they are going to Muslim Web site.

Senator JOHNSON. Mr. Swire, would you like to comment on that?

Mr. SWIRE. A lot of good things have been said. One other part of the privacy fair practice is accessing your data and correcting mistakes.

So, if you are on the no-fly list and you should not be or your credit history is wrong, they have the wrong person with your name, having good procedures around that is another part of what we consider as privacy protection that I think we surely want to build into our information society.

Senator JOHNSON. Thank you.

Thank you, Mr. Chairman.

Senator AKAKA. Thank you very much, Senator Johnson.

Mr. Calabrese, you testified that the exemptions to the Privacy Act for law enforcement and intelligence activities are problematic.

Given the many recent privacy concerns about the treatment of personal information in the national and homeland security context, I agree that this issue merits further examination.

How can we ensure that these exemptions are not abused without harming important law enforcement and intelligence activities?

Mr. CALABRESE. Thank you, Senator,

Well, I think in terms of tightening controls, I think we can begin by acknowledging that the Privacy Act actually has pretty good disclosure limitations that says, you should not disclose information unless you have a good reason to do so.

What we need to do is tighten some of the exceptions like routine use that allows essentially anything to be labeled routine and hence disclosed.

And, I think that goes to the heart of how we get both a strong national security and also good privacy is we need to focus our investigations on people we suspect of wrongdoing, who are criminals, who are terrorists.

When we have a basis for that investigation, we pursue it. There are plenty of mechanisms for doing so. That does not mean compiling a database of all the innocent people in advance in case they may some day be needed for this.

When we have an investigation we pursue it. We do not put every American in what amounts to a lineup on the assumption that someday that lineup may prove valuable.

One of our enduring rights in this country is that we are innocent until proven guilty. We need to hold onto that bedrock principle. Thank you.

Senator AKAKA. Thank you.

Mr. Rosenzweig and Mr. Calabrese, I agree with Mr. Swire that approving the nominees for the Privacy and Civil Liberties Oversight Board is a critical priority, particularly as the Senate considers cybersecurity legislation.

As you know, the Board is supposed to be a key check on the new information sharing authorities in the bill. I would like to hear your views on this issue.

Let me call on Mr. Swire first.

Mr. SWIRE. I think I spoke to it, sir. I am not sure I have more to add to the idea that we should get these folks confirmed.

Senator AKAKA. Thank you. Mr. Rosenzweig.

Mr. ROSENZWEIG. I do not know all of the nominees. The three that I know are quite able. I would have hoped that the Senate would have acted with President Bush in 2007 to fill the Board and I would have hoped that President Obama, if he had acted with more alacrity and presented these nominees well before the near end of this session, we would have had a Board in place.

I agree completely that at some point a Board needs to be put in place because, as I said, I think that the oversight and audit functions are critical to my vision of the best ways to enhance privacy. I just regret that the political dimension of this has brought us to the point where we are, what, 98 days out from an election and still trying to find a Board.

Senator AKAKA. Thank you. Mr. Calabrese.

Mr. CALABRESE. I agree obviously. We want to confirm these nominees tomorrow, if possible.

I want to just caution, though, it is not a panacea. I mean PCLOB is relatively small, even if it was fully staffed, it is something like 10 full-time staff under its current budget allotment. A part-time Board with a full-time chairman.

The agencies and the bureaucracies that it is supposed to oversee are quite literally massive. They are the size of small towns. So, there is no way that this Board is going to be able to provide any level of complete oversight.

It is a piece. It is necessary to fill it but no one should believe that simply filling the PCLOB is going to answer all our oversight concerns.

Senator AKAKA. Thank you.

Mr. Swire, if we create a Federal Chief Privacy Office, should that individual also review the information sharing provisions of the cybersecurity bill?

Mr. SWIRE. So, how to work the CPO with the PCLOB is something that would take some work. I suggest in my testimony that we have a long-held decision between unclassified commuter systems in the Federal Government and the classified systems.

The Privacy and Civil Liberties Oversight Board is specifically focused on classified and anti-terrorism activities. It makes sense I think for them to take the lead there and for the Federal Chief Privacy Officer to take the lead on unclassified systems. That is my best guess at how to proceed.

Senator AKAKA. Thank you.

This is my final question for the entire panel. What key privacy protection issues that we have not yet discussed also warrant the attention of Congress? Mr. Calabrese.

Mr. CALABRESE. There are so many. I would say that it is really crucial to update our electronic communications privacy laws (ECPA). For example, ECPA was passed in 1986. It governs law enforcement access to electronic communications.

It is woefully out of date. 1986 was an awful long time ago. Similarly location privacy, as the court weighed in *US v. Jones* this term, is a huge issue. Our cell phones have become portable tracking devices, and reining in that tracking so it only happens appropriately I think is a very important job.

I could go on and on but I will stop at those two.

Senator AKAKA. Thank you. Mr. Rosenzweig.

Mr. ROSENZWEIG. Those two are both worth thinking about. I guess I would add to that a consideration of whether or not the intelligence community's approach to privacy is sufficiently unified. I think there is divergency in views within that community.

And, wow, I could probably think of a half dozen more but I will just stop with that.

Senator AKAKA. Mr. Swire.

Mr. SWIRE. So, just two observations. One is that the Jones case about tracking the location I think is a very important moment for the Supreme Court but Congress can followup there.

I did a project with some other groups at *U.S. v. Jones.com* which surveys ways to sort of get out the next generation of surveillance and civil liberties here. I think I would focus on that, how to do the electronic searches, how to update ECPA, and how to do some of the things discussed at *US v. Jones.com*.

Senator AKAKA. Thank you. Let me ask Senator Johnson for further questions.

Senator JOHNSON. Thank you, Mr. Chairman.

Let me just address the very real conundrum facing government. As we watch every terrorist act, the aftermath of that, people start doing a postmortem on that, and they go, well, we had this information, why did we not put two and two together and prevent the attack.

A very real concern, and it is just that natural tension between privacy and the security that the American people expect. I guess I would like all three of you to, first of all, address that very real concern to me. How do we navigate that very fine line?

I guess we will start with Mr. Swire.

Mr. SWIRE. Thank you, Senator.

So, I wrote a law review article around 2006 called Privacy and Information Sharing in the War Against Terrorism. It is online and law professors always love it if anybody ever reads a law review article.

But I think that is a checklist of seven or eight questions that I think should be asked as you are building a new information system. And, it actually is similar to what Mr. Rosenzweig is saying about audit and accountability and setting it up so someone is looking at it carefully when you built it at the front and then auditing it once you have it in place.

And, I think if you do that, then you do use information intensively but you have some safeguards in place.

Senator JOHNSON. Thank you. Mr. Calabrese.

Mr. CALABRESE. Well, I think one of the biggest problems with information sharing today is that there is so much information that it overwhelms the ability of any analyst to essentially process it.

I mean, you cannot connect the dots when it is millions of dots being given to you every day. I mean, Secretary Leiter, when he was the Director of the NCTC, talked about an amazing amount of leads and tips that they get every day.

And so, I think that we need to try to weed out the innocent person chaff and focus more on actual leads, actual people who, when Abdulmutallab's father came in to the Embassy and said, please investigate my son, it certainly seems possible to me that lead became lost because there was so much information pouring in that a good lead was lost amongst all the chaff.

I think we need to focus on narrowing our information sharing to the right information, and that is a difficult task but I think one that will bear the most fruit.

Senator JOHNSON. Mr. Rosenzweig.

Mr. ROSENZWEIG. I actually have a different perspective on that which is I agree that we are drowning in a flood of data, but to a large degree our capacity to analyze it has been hamstrung by our unwillingness to apply data analytics.

Abdulmutallab was actually a good example because the father coming in was preceded apparently by a visa application that would have been in the field of innocent data, presumptively innocent data that was collected about all of these applicants.

You cannot know ex-ante which data fields are going to be the ones that are relevant to an ongoing investigation. Up until just a

couple of years ago, we actually did not have a coordinated Google-like search functionality within the intelligence community, not because we could not implement that, though it does take some money and coordination, but in part because we were concerned about the linkages between various databases as eroding privacy concerns.

When you have those concerns at the front end, they sometimes create artificial limitations. I agree completely that the right answer is to try to use the analytics to narrow down leads into the people that we want to devote investigative resources to. That is precisely what all of these systems are intended to do.

On the other hand, you cannot actually make them as effective as you might by limiting the intake on the front-end.

So, my perspective is that we are always going to be doing too much until the day after an event when we will not have done enough, and the optimal answer is to try to get the right structures in place up-front and at least be able to defend your choices going forward.

Senator JOHNSON. Mr. Calabrese, I will definitely side with people who are highly concerned about civil liberties and government intrusion into our lives.

Can you, describe specific examples of purposeful misuse by the government of some of the information, personal privacy information as opposed to hackers getting in and information being not purposefully but illegally disclosed?

Mr. CALABRESE. Yes. Let me address your question first, Senator. I think we saw with the New York Police Departments (NYPD's) investigation of Muslim communities where they were, they began to surveil entire communities, do community mapping of Muslims, not because they had any particular belief that there was a particular person who they need to investigate but just simply to monitor the entire community.

Similarly we have seen reports, and the ACLU has done FOIAs on this, where FBI agents under the guise of going and doing community outreach and just getting to know the Muslim community, something that I think everybody agrees is vital in terms of building bridges and connections so that they will feel free to come forward if there is a criminal issue, were turned into intelligence reports where reports were compiled on those innocent people who were trying to help the government do community outreach.

So, when we turn people who are trying to help us into suspects, it builds exactly kind of distrust that we are trying to prevent and I would argue hinders investigations going forward.

So, I think that is the kind of situation that we want to prevent and that is why we want to preserve some of the lines that we have been talking about.

Senator JOHNSON. That is somewhat kind of outside what we are talking about here, at least what I am talking about in terms of privacy within the cyber community.

Mr. Rosenzweig, you mentioned Google. I mean, Google has all the information. If you have a credit card, you have provided voluntarily all kinds of personal information. And, I guess, I just want somebody to speak to the disconnect between what we voluntarily give up to private companies that have a great deal of latitude, al-

most primordial latitude for use and misuse of that information in the Federal Government.

Can you just kind of speak to that disconnect?

Mr. ROSENZWEIG. Well, there is much to be said about Google's privacy policies which many people think are not strong enough in the private sector. I think the best way to characterize it would be this.

Just this past week in Las Vegas, they had the Black Hat convention DEFCON which is a convention of hackers. And, one of the leaders of the audience asked this assembled group of true cyber experts who they feared more, Google's privacy invasions or the government's, and Google won hands down, because the people with the knowledge about this know that Google actually assembles, processes, and uses personal data much more efficiently, much more effectively than the Federal Government does.

So, if you are one who sees in that a threat, as the people at DEFCON did, they are more afraid of Google than they are of the government by I think it was like six to one I saw in the newspapers. I obviously was not there but that kind of speaks to it.

Senator JOHNSON. Thank you. I have run out of time again. I really do want to thank the witnesses for your thoughtful testimony and taking the time here. This has been a very interesting discussion and, Mr. Chairman, for holding this hearing. This is a good hearing.

Senator AKAKA. Go ahead.

Senator JOHNSON. No. I think I am good. Thank you.

Senator AKAKA. Well, thank you very much, the second panel. I would like to thank each of you for your statement and your responses. This has been a useful and informative discussion that will help us chart the next steps to strengthen our Federal privacy and data security framework. I will continue focusing on these important issues during the rest of my time in the Senate.

This hearing also will provide a blueprint for the next Congress on additional areas that must be addressed.

The hearing record will be open for 2 weeks for additional statements or questions from members of this Subcommittee.

Again, I want to thank you for being with us.

The hearing is adjourned.

[Whereupon, at 11:58 a.m., the Subcommittee adjourned.]

A P P E N D I X

STATEMENT OF CHAIRMAN DANIEL K. AKAKA

State of Federal Privacy and Data Security Law: Lagging Behind the Times?

Hearing
Subcommittee on Oversight of Government Management,
the Federal Workforce, and the District of Columbia,
Senate Committee on Homeland Security and Governmental Affairs

I call this hearing of the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia to order. I want to welcome our witnesses. Aloha and thank you for being here.

Today, the Subcommittee will examine the foundation for our federal privacy and data security laws. Unfortunately, key pieces of this foundation have serious cracks that need to be fixed.

The Privacy Act, a cornerstone of federal privacy protection, was enacted in 1974 to respond to the increasing ease of collecting and storing personal information in computer databases. It governs how the federal government gathers, shares, and protects Americans' personal information.

Despite dramatic technological change over the last four decades, much of the Privacy Act remains stuck in the 1970s. Many of the definitions in the Act are simply out of date and do not make sense in the current data environment. As a result, the Act is difficult to interpret and apply, and it provides inconsistent protection to the massive amount of personal information in the hands of the government. I want to highlight a few specific concerns.

Earlier this year, the Supreme Court restricted Privacy Act remedies. In Federal Aviation Administration v. Cooper, the Social Security Administration violated the Privacy Act by sharing the plaintiff's HIV status with other federal agencies. The Court concluded that he could not be compensated for emotional distress, because Privacy Act damages are limited to economic harm. By many experts' accounts, this decision rendered the Act toothless, and scholars across the political spectrum have called for Congress to amend the Privacy Act to fix this decision.

Additionally, agencies frequently use private sector databases for law enforcement and other purposes that affect individuals' rights. This is not covered by federal privacy laws, which creates a loophole that allows agencies to avoid privacy requirements. We should require privacy impact assessments on agencies' use of commercial sources of Americans' private information. This would provide basic transparency of agencies' use of commercial databases, so that individuals have appropriate protections such as access, notice, correction, and purpose limitations.

Strong executive branch leadership is also essential to effectively enforcing the privacy protections we do have. Over time, Congress has statutorily required Chief Privacy Officers in many agencies across the federal government, and the Office of Management and Budget (OMB) mandated in 1999 that all agencies designate a senior privacy official to assume responsibility for privacy policy. My Privacy Officer With Enhanced Rights (POWER) Act – included in the Implementing Recommendations of the

9/11 Commission Act of 2007 – strengthened the authorities of the DHS Chief Privacy Officer, with positive results.

Despite OMB's mandate to oversee privacy policies government-wide, it has not named a chief privacy official since the Clinton Administration. As a result, responsibility for protecting privacy is fragmented and agencies' compliance with privacy requirements is inconsistent.

Widespread agency data breaches, and inconsistent responses when they occur, are symptoms of this problem. We all remember the massive data breach at the Department of Veterans Affairs in May 2006, where the personal information of more than 26 million veterans and active duty members of the military was exposed. After that breach, OMB issued guidance in 2007 requiring agencies to strengthen safeguards for personal information and implement data breach notification policies. But implementation of the guidance has been uneven, and the number of federal data breaches has only grown.

Recently, a contractor to the Federal Retirement Thrift Investment Board was the subject of a cyber attack that compromised the personal information of over 123,000 participants in the Thrift Savings Plan. This included 43 current and former Members of Congress. I was concerned to learn that the Board had not followed the 2007 OMB guidance and did not have a data breach notification policy in place when they learned of the breach. I am working with the Government Accountability Office (GAO) to determine how many other agencies have not followed this guidance and determine whether there is sufficient oversight of agencies that have complied.

This builds on the substantial work GAO has completed in response to my nine previous requests on privacy and data security. I have also worked closely with GAO in drafting my Privacy Act Modernization for the Information Age Act (S. 1732), which would make the OMB guidance mandatory for agencies and fix many of the other cracks in the privacy and data security foundation.

Promoting privacy and civil liberties has been a priority during my tenure in the U.S. Senate, and I will continue focusing on this issue until the end of the year. I hope my colleagues will join me in two current efforts to address the problems raised at this hearing: S. 1732 and my amendment to the Cybersecurity Act of 2012 (S. 3414), which we are currently considering on the Senate floor. Protecting Americans' privacy is a bipartisan issue that I hope my colleagues will continue to advance in the years to come.

-END-

HEARING OPENIGN STATEMENT OF SENATOR TOM CARPER

**“State of Federal Privacy and Data Security Law: Lagging Behind the Times?”
Subcommittee on Oversight of Government Management, the Federal Workforce, and the
District of Columbia
July 31, 2012**

I would like to thank Chairman Akaka and Ranking Member Johnson for holding this very important hearing on our nation’s privacy and data security laws. Protecting individual privacy is of critical importance.

A few months ago, many Americans were very troubled to learn that a contractor for the Federal Retirement Thrift Investment Board suffered a major cybersecurity attack, which exposed the personal information of more than 123,000 Thrift Savings Plan participants. This breach, and the many others like it in both government and the private sector, highlight the need for Federal data security standards. The need for strong measures against privacy breaches is a clear reason why we are debating cybersecurity legislation on the Senate floor right now.

The Cybersecurity Act of 2012, which I was proud to co-author with Chairman Lieberman, Ranking Member Collins, and Senators Rockefeller and Feinstein, takes a number of bold steps to better secure our critical infrastructure and government networks. This bill is not perfect, but it represents a dramatic improvement over current law. It is also a good-faith effort to address the concerns of Members on both sides of the aisle.

By passing this bill we will help usher in a new generation of cyber tools for the federal government so that government agencies, such as the Thrift Investment Board, can be better prepared to face the cyber challenges of the 21st century.

As we have learned from the Thrift Savings Plan case, we must do more to ensure that sensitive consumer information is properly protected, and timely notification to consumers is provided in the event of a breach. Fraud and identity theft have serious consequences, and it is time we make sure government agencies, companies and others handling this sensitive information have rules in place to safeguard this information.

For several years now, I have introduced bipartisan legislation, and now which is filed as an amendment to the cybersecurity bill, to ensure these safeguards are established and implemented. This hearing highlights a very serious problem with regards to data security and I hope we can use the challenges highlighted by the Thrift Savings Plan case and others like it, to establish national data security standards.

WRITTEN TESTIMONY

of

MARY ELLEN CALLAHAN

CHIEF PRIVACY OFFICER

DEPARTMENT OF HOMELAND SECURITY

Before the

UNITED STATES SENATE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT MANAGEMENT

Release Date: July 31, 2012

Good morning, Chairman Akaka, Ranking Member Johnson, and Members of the Subcommittee. I appreciate the opportunity to appear before you today to discuss my role as the Department of Homeland Security's (DHS) Chief Privacy Officer, the Privacy Act, and the collaborative achievements of the Privacy Committee of the Federal Chief Information Officers Council.

Role of the DHS Chief Privacy Officer

As you know, the Department of Homeland Security (DHS) is the first department in the federal government to have a statutorily mandated privacy officer. I have had the pleasure of serving in this role since March 2009. The Homeland Security Act grants the Chief Privacy Officer primary responsibility for ensuring that privacy considerations and protections are comprehensively

integrated into all DHS programs, policies, and procedures.¹ Pursuant to my statutory authority, I am tasked with assuring that the Department's use of technologies sustains and does not erode privacy protections relating to the use, collection, and disclosure of personal information. I also ensure that personal information contained in Privacy Act systems of record is handled in full compliance with fair information practices, as set forth in the Privacy Act of 1974, as amended.² To achieve this mandate, I lead a dedicated staff of privacy professionals who comprise the DHS Privacy Office.

The mission of the DHS Privacy Office is to protect all individuals by embedding and enforcing privacy protections and transparency in all DHS activities. My staff work to achieve its mission by fostering a culture of privacy and transparency; demonstrating leadership through policy and partnerships; providing outreach, education, training, and reports; conducting robust oversight; and ensuring that DHS complies with federal privacy, confidentiality, and disclosure laws, policies, and principles.

It is my pleasure to share with you today a few examples of the DHS Privacy Office's many recent achievements in privacy protection. Last year, we issued Department Directive 047-01, which formalizes the privacy-related responsibilities of DHS personnel and the processes in place to ensure compliance with applicable laws and policies. Two weeks ago, we hosted a successful public meeting of the DHS Data Privacy and Integrity Advisory Committee, which provides advice on privacy-related matters to the Chief Privacy Officer and the Secretary of Homeland Security. In addition, we engage in ongoing collaboration with the DHS Office for

¹ 6 U.S.C. § 142.

² 5 U.S.C. § 552a.

Civil Rights and Civil Liberties to provide comprehensive, on-site training to fusion centers from Alaska to Tennessee.

Many of my authorities are similar to those of other federal Chief Privacy Officers. I am unique, however, in that my statutory mandate also includes the authority to investigate Department programs and operations; to issue subpoenas to non-federal entities; and to administer oaths, affirmations, and affidavits necessary to conduct investigations. During my tenure, I have led three investigations of significant non-compliance with Departmental privacy policy. One investigation concerned a privacy incident involving loss of an unencrypted flash drive with financial audit data that contained Sensitive PII. In February 2011, I published a report detailing my findings and setting forth proactive recommendations to prevent and mitigate similar privacy incidents.³

The second investigation involved a Component's use of social media for operational purposes without appropriate oversight or privacy protections. After determining that the Component's use of social media was not in compliance with Department privacy policy, my Office provided the Component a set of recommendations that we then used to develop a Department-wide Directive on privacy and social media and the Component has since been in compliance.⁴ Additionally, the Directive and its associated Instruction detail specific steps Components must take before engaging in the operational use of social media, including documenting their authority, providing annual training to authorized employees, and creating specific authority-based Rules of

³ U.S. Department of Homeland Security, Privacy Office, *OIG Privacy Incident Report and Assessment* (February 2011), <http://www.dhs.gov/xlibrary/assets/privacy/priv-oig-privacy-incident-report-assessment-022011.pdf>.

⁴ U.S. Department of Homeland Security, *Privacy Policy for Operational Use of Social Media, Directive 110-01* (June 8, 2012), http://www.dhs.gov/xlibrary/assets/foia/110-01-001_Privacy_Policy_for_Operational_Use_of_Social_Media.pdf.

Behavior. This investigation improved awareness of privacy concerns and resulted in my Office providing improved standards for operational use of social media to the entire Department.

My third and most recent investigation was prompted by a referral from the DHS Office of the Inspector General. Following the referral, I initiated the investigation in order to determine whether a DHS Component's information sharing pilot with an external agency complied with DHS privacy policy and the Privacy Act and my office recently concluded this investigation.

My office remains vigilant and I use my investigatory authority judiciously and thoughtfully. We consider investigations when my privacy authority is impacted, or when the Department as a whole can establish best practices, as occurred with social media. We thoroughly examine potential violations of Department privacy policy and will not hesitate to invoke my investigative authority where warranted.

Consistent with the Office's unique position as both an advisor and an oversight body for the Department's privacy-sensitive programs and systems, I recently approved the creation of a new Privacy Oversight group within the DHS Privacy Office. This group is dedicated to monitoring, investigating, and otherwise conducting robust oversight of DHS activities to ensure compliance with Department privacy policy. In addition to conducting investigations of privacy non-compliance, the Oversight team has instituted a series of Privacy Compliance Reviews to improve a program's ability to comply with assurances made in Privacy Impact Assessments, System of Records Notices, and formal information sharing agreements. Privacy Compliance

Reviews may result in recommendations to a program, updates to privacy documentation, informal discussions on lessons learned, or a formal internal or publicly available report.

One specific example of my office's privacy efforts that you requested I discuss today is our response to the Office of Management and Budget's (OMB) guidance on safeguarding personally identifiable information (PII). OMB Memorandum M-07-16 required agencies to develop and implement a policy on breach notifications, which DHS refers to as privacy incidents.⁵ In September 2007, in response to the OMB memo, the DHS Privacy Office distributed its *Privacy Incident Handling Guidance* throughout the Department to inform employees of their responsibilities to safeguard PII, regardless of format.⁶ In addition, the *Privacy Incident Handling Guidance* provided detailed information on how to handle all stages of privacy incidents, including reporting, escalation, investigation, mitigation, notification, and closure.

The Department continues to actively implement OMB Memorandum M-07-16. Earlier this year, my Office revised its *Privacy Incident Handling Guidance* to better reflect privacy incident handling procedures based on observed best practices.⁷ We also issued a *Handbook for Safeguarding Sensitive Personally Identifiable Information*, which establishes minimum standards for how Department personnel should protect Sensitive PII.⁸ To ensure that staff are

⁵ OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007).

⁶ Information may exist in paper, electronic, web-based, or other formats, for example.

⁷ U.S. Department of Homeland Security, *Privacy Incident Handling Guidance* (Revised January 26, 2012), http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf.

⁸ U.S. Department of Homeland Security, *Handbook for Safeguarding Sensitive Personally Identifiable Information* (March 2012), <http://www.dhs.gov/xlibrary/assets/privacy/dhs-privacy-safeguardingsensitivepiihandbook-march2012.pdf>.

cognizant of PII protections, we also updated our annual online training, which is mandatory for all DHS employees and contractors.

The Privacy Act of 1974

The Privacy Act was passed in an era before electronic communications and databases were the norm at federal agencies. As such, the Act did not fully contemplate that multiple entities within the Executive Branch may use the same types of records or operate similar systems. Nonetheless, many of the concepts embedded in the original Act are flexible enough to permit similar records to be treated consistently, regardless of whether they are located at one agency or another. One example of this is the government-wide Systems of Records Notices (SORN), which was developed by the Office of Personnel Management to cover all personnel records across the Executive Branch and ensure that they are treated consistently. DHS employs a similar practice of treating like records consistently under the Privacy Act. For security personnel records, for example, DHS has a single SORN to ensure consistent treatment, regardless of which component maintains the record. DHS also has a single SORN for all Department contact lists regardless of the list's location or format. The practices described above promote efficiency and Privacy Act compliance, while ensuring that the public understands how information is used and stored.

Privacy Committee of the Federal Chief Information Officers Council

One method to address modern challenges of implementing the Privacy Act is to share best practices among federal privacy officials. Formal Council-level bodies exist for many federal chief officers, including the Chief Financial Officers, Chief Information Officers, and Chief Human Capital Officers. Though no formal Council-level body exists for Chief Privacy Officers,

I am proud to serve as Co-chair of the Privacy Committee of the Federal Chief Information Officers Council.

The Privacy Committee was initially formed in response to the need to coordinate on shared challenges, such as information sharing and protection of personally identifiable information. Since its formal establishment in 2009, the Committee has successfully functioned as a consensus-based forum for the development of privacy policy and protections throughout the federal government. The Committee currently serves as the interagency coordination group for federal Chief Privacy Officers and Senior Agency Officials for Privacy. It provides an important venue in which to share experiences, training, innovative approaches, best practices, and safeguards with other federal privacy professionals.

One example of how the Committee has benefited the federal privacy community at large is through its interagency training sessions. In the first year of the Administration, the Committee hosted a privacy training “boot camp” for new senior privacy officials to enhance their ability to promote privacy protection in their respective agencies. The Committee has shared additional knowledge and first-hand experience with the privacy community, including public stakeholders, through three plenary Summits and focused events on international privacy and other timely topics.

In addition to hosting government-wide training, the Committee has led development of privacy standards and safeguards for emerging technologies, such as cloud computing and social media. The Committee seeks opportunities to promote privacy through partnership with other federal

entities, such as the National Institute of Standards and Technology (NIST). The latest draft of NIST's security guidance, which applies to information systems across the federal government, reflects the joint development of comprehensive privacy controls informed by the Committee's extensive privacy expertise.⁹ The achievements of the Privacy Committee indicate the vital role it serves in promoting consistent federal privacy policy, and it has been an honor to serve as one of the Committee's chairs.

Conclusion

The efforts of the Privacy Committee and of the DHS Privacy Office benefit greatly from the support of this subcommittee and its members. Going forward, I am confident that the Department will continue to embed privacy and confidentiality protections throughout its programs and systems. I am happy to answer any questions you may have.

#####

⁹ U.S. Department of Commerce, National Institute of Standards and Technology. *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, Revision 4, Initial Public Draft (February 2012), <http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf>.

**STATEMENT OF GREGORY T. LONG EXECUTIVE DIRECTOR FEDERAL
RETIREMENT THRIFT INVESTMENT BOARD BEFORE THE SUBCOMMITTEE
ON OVERSIGHT OF GOVERNMENT MANAGEMENT, THE FEDERAL
WORKFORCE AND THE DISTRICT OF COLUMBIA JULY 31, 2012**

Good morning, Chairman Akaka and members of the Subcommittee, my name is Greg Long and I am the Executive Director of the Federal Retirement Thrift Investment Board (FRTIB). The five members of the Board and I serve as the fiduciaries of the Thrift Saving Plan (TSP). As fiduciaries, the law directs that we act solely in the interest of the TSP's participants and beneficiaries and exclusively for the purpose of providing them with benefits. Because of this fiduciary duty, in the Federal Employees' Retirement System Act (FERSA), Congress afforded the FRTIB significant independence. The FRTIB does not receive appropriated funds for its operations. We are funded through participant monies and our budget is not subject to review or approval by Congress or the President.

The TSP is the largest defined contribution retirement plan in the world. Individual accounts are maintained for more than 4.5 million Federal and Postal employees, members of the uniformed services, retirees, and spousal beneficiaries. As of June 30, 2012, the TSP held approximately \$313 billion in retirement savings.

I have been asked to discuss a number of issues, including the cyber attack that resulted in the unauthorized access of the personally identifiable information of roughly 123,000 TSP participants and payees. In July of 2011, a desktop computer used by an employee of Serco, Inc. was subjected to a sophisticated cyber attack. Serco is a contractor which assists with TSP record keeping – keeping track of participant accounts and funds. Neither Serco nor the FRTIB was aware of the attack at the time it occurred.

In April 2012, the Federal Bureau of Investigation (FBI) notified Serco that the FBI had discovered data that appeared to be stolen from Serco. On April 10, 2012, Serco notified the FRTIB of the cyber attack. On that day, Serco told the FRTIB that Serco's system had been compromised, but Serco did not yet have knowledge of whether any data belonging to FRTIB had been accessed. The FRTIB and Serco immediately acted to isolate and contain the personal computer that was the suspected source of the data.

On April 13, after a combined investigation, the FRTIB and Serco determined that data belonging to FRTIB, including personally identifiable information of TSP participants and payees, had been compromised. As required by the Federal Information Security Management Act (FISMA), within one hour of the discovery, the FRTIB notified US CERT at the Department of Homeland Security. At that time, however, the FRTIB did not yet know which participants and payees were affected by the incident.

The FRTIB and Serco worked together to analyze numerous files and, by May 4, had compiled an unverified list of Social Security numbers and, in some instances, other information (e.g., TSP account numbers) that had been compromised. No names were associated with the majority of these Social Security numbers. On May 8, the FRTIB produced a file that had been verified against the TSP participant database.

On May 20, an independent verification and validation (IV&V) concluded that the various files that had been accessed from the Serco computer had been completely and correctly analyzed to accurately capture the affected population.

On May 25, five days after the final, complete list was produced, the FRTIB notified affected participants and other stakeholders about the cyber attack. The FRTIB sent letters to every affected participant notifying them of the cyber attack, the fact that certain personally identifiable information had been accessed, and offering them one year of free identity theft consultation, restoration, and continuous credit monitoring.

I would like to emphasize the fact that this cyber attack was made on our contractor's network. Neither the FRTIB's network nor the TSP participant website www.tsp.gov was affected. I would also like to emphasize that we have no reason to believe that this data has been misused.

Nonetheless, we undertook a comprehensive review of our systems to ensure that they had not been affected. Serco also took a variety of steps to address the cyber attack. The immediate response included initiating scans and sweeps of devices, deploying additional event detection devices, and delivering awareness training to Serco employees. Serco then conducted a forensic analysis on the target hard drive to determine whether malware was present, coordinated a review and feedback from the FBI on the hard drive, and had an external forensics review of the hard drive. Serco next completed an information technology assessment and completed its scanning of its computer systems.

Operationally, we have over a long period of time provided specific guidance to Serco and worked with them to implement controls and processes to protect FRTIB enterprise-wide hardware, software, and information assets. Examples of these controls and processes include standard security configurations for server, database, and network platforms, defining and implementing requirements for firewall security practices, and implementing requirements for the control of ports on devices at our call centers.

As the fiduciary for a plan charged with protecting the retirement savings of more than 4.5 million participants and beneficiaries, data security and privacy protection are priorities for me and the employees of the FRTIB. Over the past decade, the FRTIB has undertaken a significant number of changes in both its infrastructure and the features offered through the TSP. The FRTIB transitioned from the Department of Agriculture's National Finance Center to private contractor support for its record keeping operations. That transition was completed in 2006. From 2008 through 2011, the FRTIB engaged in a substantial information technology (IT) modernization effort, which included a change in data centers. The FRTIB has been keenly focused on upgrading its infrastructure and security during this time. We have created new call centers, instituted a back-up data center to ensure continuity of operations, updated our record keeping software, purchased a new mainframe, developed disaster recovery plans and testing for those recovery plans, mainframe and distributed systems, modernized the network, including full redundancy and high availability, initiated a virtual infrastructure, and deployed a new www.tsp.gov website. These efforts speak to major IT or IT support activities that provided technical controls to improve our IT security posture.

In addition to these infrastructure enhancements, over the past decade, in many cases in response to legislation, the FRTIB has successfully added new services for its participants and beneficiaries: daily valuation of participant accounts; catch-up contributions for participants 50 years of age and older; life cycle funds; immediate contributions for newly-hired Federal employees; auto-enrollment for newly hired Federal employees; beneficiary accounts for spouses of deceased TSP participants; annual participant statements; accounts for uniformed services; and, most recently in May of 2012, a Roth TSP option, allowing for after-tax contributions to the TSP.

Many of these changes added significant complexity to the Plan. The infrastructure changes listed above were necessary, in many cases, to allow the FRTIB to offer these new services to TSP participants. The need to implement these new funds and services, in large part, mandated how we assigned our personnel and allocated funding. For example, rolling out the Roth TSP initiative was a two-year project that required staffing from every office within the Agency. The complexity of the programming necessitated that we delay other programming changes to ensure a stable platform to allow for the success of Roth. We also had to revise virtually every form, notice, and brochure that we have – more than 145 – to reflect the new Roth option. As a result of this careful planning and prioritization of effort, the Roth TSP rollout was successful.

I was also asked to address the Agency's compliance with the Privacy Act and the E-Government Act. The FRTIB complies with the Privacy Act and has implemented the security controls and incident prevention processes, consistent with the data and systems held by our agency, as spelled out in FISMA. Because we are not covered by the Transportation, Treasury, Independent Agencies, & General Appropriations Act of 2005, the FRTIB is not required to appoint a Chief Privacy Officer, and, therefore, has not. The Agency's Office of General Counsel is responsible for ensuring compliance with the Privacy Act.

While the FRTIB has security controls in place, completing all of the documentation and accreditation that FISMA requires is an on-going area of focus for our Agency. I recognize that a comprehensive IT security management program is of paramount importance to the Board and we are making strides toward that goal. In September 2011, the FRTIB issued an Enterprise Information Security and Risk Management (EISRM) directive. Its purpose is to ensure that the FRTIB information systems operate with an acceptable level of risk. Its scope is all information resources used or operated by the Agency, an Agency contractor or any other organization on behalf of the Agency to access, collect, create, record, process, transmit, store, retrieve, display, print, or otherwise disseminate information owned or maintained by the Agency. The EISRM program has four major components: 1) key roles and responsibilities; 2) a risk management framework; 3) policies and controls; and 4) standards, procedures, and guidance.

As part of the continued implementation of the EISRM program, on June 29, 2012, I approved policies covering 18 families of management, operational, and technical security controls. To ensure that our privacy and data security policies are appropriate, I have commissioned a “Tiger Team” to develop a plan to improve the security posture of information systems that contain Agency information. The Tiger Team has four main objectives:

- Assess the current state of implementation of information security controls against FRTIB Enterprise Information Security and Risk Management (EISRM) requirements;
- Assess the current state of FRTIB’s application and infrastructure security architecture and data;
- Assess the current state of outstanding findings; and then
- Develop a plan to address any identified gaps. Where practical, the team will address gaps within their respective areas in compliance with the EISRM requirements.

I regret to say that the FRTIB did not have a breach notification plan in place prior to 2012. This was due to a lack of resources to develop the plan. As noted above, the past decade has been a time of dramatic expansion for the Agency, in the number of participants, the dollars invested in the TSP and the services provided to our participants and beneficiaries. This growth taxed the Agency’s ability to complete all that needed to be done. During the FRTIB response to the cyber attack, I placed our General Counsel, in charge of the breach response team. In turn, the General Counsel instructed the team to use the May 22, 2007 OMB guidance as a roadmap for the team working to respond to the cyber attack. The team found the OMB guidance very useful and information in the guidance helped expedite the FRTIB response to the attack. I have since signed the FRTIB’s breach notification plan on June 14, 2012.

As for instances of inter-agency sharing of knowledge, the FRTIB shares security and privacy materials with other agencies on an ad hoc basis. It also participates in groups like the Small Agency General Counsel consortium, the CIO Small Agency Council and the Chief Information Security Official (CISO) Advisory Council. We also participate in non-Federal associations, such as the National Association of Public Pension Plan Attorneys, in order to learn about other government retirement plans’ best practices in areas like security and privacy.

I was asked whether the FRTIB has any recommendations to improve privacy laws. My suggestion is not directed at the Privacy Act, per se, but at a problem specific to the FRTIB. Currently, FERSA does not contain a statute of limitations for judicial review of a claim for benefits brought by a TSP participant or beneficiary. This indefinite exposure to potential litigation over benefits forces the TSP to retain records of benefits paid for an unlimited period of time, even after a participant's account balance has been completely disbursed and he or she is no longer a participant. The absence of a statute of limitations, therefore, results in an extraordinary record retention burden, which increases the data potentially available to be accessed through a cyber attack or other data breach.

We, therefore, suggest that FERSA be amended to create a five year statute of limitations on judicial review of a claim for benefits. This would be longer than the statute of limitations available to virtually all plans covered by the Employee Retirement Income Security Act of 1974 (ERISA). Under ERISA, courts have ruled that as little as 90 days, 3 years and 39 months were reasonable statutes of limitations for private sector employee benefit plans.

Mr. Chairman and members of the Subcommittee, helping people retire with dignity is what drives the employees of the FRTIB. Congress made it clear that we are a unique agency with the mission of administering the TSP solely in the interest of the participants and beneficiaries. We take this very seriously. I deeply regret the cyber attack and the concern that it caused our participants. I want to take this opportunity to assure all of our participants and beneficiaries that we will continue to pursue all new avenues of data and computer security to ensure the safety and security of their personal data and their retirement funds.

United States Government Accountability Office

GAO

Testimony
Before the Subcommittee on Oversight of Government
Management, the Federal Workforce, and the District of
Columbia, Committee on Homeland Security and
Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. EDT
Tuesday, July 31, 2012

PRIVACY

Federal Law Should Be Updated to Address Changing Technology Landscape

Statement of Gregory C. Wilshusen, Director
Information Security Issues



July 31, 2012



Highlights of GAO-12-961T, a testimony before the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate

PRIVACY

Federal Law Should Be Updated to Address Changing Technology Landscape

Why GAO Did This Study

The federal government collects and uses personal information on individuals in increasingly sophisticated ways, and its reliance on information technology (IT) to collect, store, and transmit this information has also grown. While this enables federal agencies to carry out many of the government's critical functions, concerns have been raised that the existing laws for protecting individuals' personal information may no longer be sufficient given current practices. Moreover, vulnerabilities arising from agencies' increased dependence on IT can result in the compromise of sensitive personal information, such as inappropriate use, modification, or disclosure.

GAO was asked to provide a statement describing (1) the impact of recent technology developments on existing laws for privacy protection in the federal government and (2) actions agencies can take to protect against and respond to breaches involving personal information. In preparing this statement, GAO relied on previous work in these areas as well as a review of more recent reports on security vulnerabilities.

What GAO Recommends

GAO previously suggested that Congress consider amending applicable privacy laws to address identified issues. GAO has also made numerous recommendations to agencies over the last several years to address weaknesses in policies and procedures related to privacy and to strengthen their information security programs.

View GAO-12-961T. For more information, contact Gregory C. Wilshusen (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Technological developments since the Privacy Act became law in 1974 have changed the way information is organized and shared among organizations and individuals. Such advances have rendered some of the provisions of the Privacy Act and the E-Government Act of 2002 inadequate to fully protect all personally identifiable information collected, used, and maintained by the federal government. For example, GAO has reported on challenges in protecting the privacy of personal information relative to agencies' use of Web 2.0 and data-mining technologies.

While laws and guidance set minimum requirements for agencies, they may not protect personal information in all circumstances in which it is collected and used throughout the government and may not fully adhere to key privacy principles. GAO has identified issues in three major areas.

- **Applying privacy protections consistently to all federal collection and use of personal information.** The Privacy Act's protections only apply to personal information when it is considered part of a "system of records" as defined by the act. However, agencies routinely access such information in ways that may not fall under this definition.
- **Ensuring that use of personally identifiable information is limited to a stated purpose.** Current law and guidance impose only modest requirements for describing the purposes for collecting personal information and how it will be used. This could allow for unnecessarily broad ranges of uses of the information.
- **Establishing effective mechanisms for informing the public about privacy protections.** Agencies are required to provide notices in the *Federal Register* of information collected, categories of individuals about whom information is collected, and the intended use of the information, among other things. However, concerns have been raised whether this is an effective mechanism for informing the public.

The potential for data breaches at federal agencies also pose a serious risk to the privacy of individuals' personal information. OMB has specified actions agencies should take to prevent and respond to such breaches. In addition, GAO has previously reported that agencies can take steps that include

- assessing the privacy implications of a planned information system or data collection prior to implementation;
- ensuring the implementation of a robust information security program; and
- limiting the collection of personal information, the time it is retained, and who has access to it, as well as implementing encryption.

However, GAO and inspectors general have continued to report on vulnerabilities in security controls over agency systems and weaknesses in their information security programs, potentially resulting in the compromise of personal information. These risks are illustrated by recent security incidents involving individuals' personal information. Federal agencies reported 13,017 such incidents in 2010 and 15,560 in 2011, an increase of 19 percent.

Chairman Akaka, Ranking Member Johnson, and Members of the Subcommittee:

Thank you for the opportunity to testify at today's hearing on the state of federal privacy and data security laws. These laws are intended to protect the privacy of Americans' personally identifiable information and specify measures that federal agencies can take to reduce the risk of breaches of sensitive personal information.

As you know, the increasingly sophisticated ways in which personal information is obtained and used by the federal government has the potential to assist in performing critical functions, such as helping to detect and prevent terrorist threats and enhancing online interactions with citizens. But these technological developments can also pose challenges in ensuring the protection of citizens' privacy. In addition, the increasing reliance by federal agencies on information technology (IT) has radically changed the way our government, our nation, and much of the world communicate and conduct business. While bringing significant benefits, this dependence on IT can also create vulnerabilities that can result in, among other things, the compromise of sensitive personal information through inappropriate use, modification, or disclosure.

In my testimony today, I will describe (1) the impact of recent technology developments on existing laws for privacy protection in the federal government, and (2) actions agencies can take to protect against and respond to breaches involving personal information. In preparing this statement in July 2012, we relied on our previous work in these areas. (Please see the related GAO products list at the end of this statement.) These products contain detailed overviews of the scope and methodology we used. We also reviewed more recent agency inspector general assessments of security vulnerabilities at federal agencies and information on security incidents from the U.S. Computer Emergency Readiness Team (US-CERT), media reports, and other publicly available sources. The work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Federal agency collection or use of personal information is governed primarily by two laws: the Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002. The Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records. The act describes a record as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier. The act defines a "system of records" as a group of records under the control of any agency from which information is retrieved by the name of the individual or by an individual identifier. The Privacy Act requires that when agencies establish or make changes to a system of records, they must notify the public through a system-of-records notice in the *Federal Register* that identifies, among other things, the categories of data collected, the categories of individuals about whom information is collected, the intended "routine" uses of data, and procedures that individuals can use to review and correct personally identifiable information.

Several provisions of the act require agencies to define and limit collection and use of personal information to predefined purposes. For example, it requires that, to the greatest extent practicable, personal information should be collected directly from the individual when it may affect that person's rights or benefits under a federal program. It also requires agencies to indicate whether the individual's disclosure of the information is mandatory or voluntary; the principal purposes for which the information is intended to be used; the routine uses that may be made of the information; and the effects on the individual, if any, of not providing the information. Further, in handling information they have collected, agencies are generally required to allow individuals to review their records, request a copy of their record, and request corrections to their information, among other things.

The E-Government Act of 2002 was passed, among other reasons, to enhance the protection for personal information in government information systems or information collections by requiring that agencies conduct privacy impact assessments (PIA). PIAs are analyses of how personal information is collected, stored, shared, and managed in a federal system.

Title III of the E-Government Act, known as the Federal Information Security Management Act of 2002 (FISMA),¹ established a framework designed to ensure the effectiveness of security controls over information resources that support federal operations and assets. According to FISMA, each agency is responsible for, among other things, providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. These protections are to provide federal information and systems with integrity—preventing improper modification or destruction of information, confidentiality—preserving authorized restrictions on access and disclosure, and availability—ensuring timely and reliable access to and use of information.

The privacy protections incorporated in the Privacy Act are based primarily on the Fair Information Practices—a set of widely recognized principles for protecting the privacy of personal information first developed by an advisory committee convened by the Secretary of Health, Education and Welfare in 1972 and revised by the Organization for Economic Cooperation and Development (OECD) in 1980. These practices underlie the major provisions of the Privacy Act and privacy laws and related policies in many countries, including Germany, Sweden, Australia, and New Zealand, as well as the European Union. They are also reflected in a variety of federal agency policy statements, beginning with an endorsement of the OECD principles by the Department of Commerce in 1981. The OECD version of the principles is shown in table 1.

¹FISMA, Title III, E-Government Act of 2002, Pub. L. 107-347 (Dec. 17, 2002), 44 U.S.C. § 3541, et seq.

Table 1: The Fair Information Practices

Principle	Description
Collection limitation	The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
Data quality	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
Purpose specification	The purposes for the collection of personal information should be disclosed before collection and upon any change to that purpose, and its use should be limited to those purposes and compatible purposes.
Use limitation	Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.
Security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
Openness	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
Individual participation	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.
Accountability	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

Source: OECD.

The Privacy Act gives the Office of Management and Budget (OMB) responsibility for developing guidelines and providing assistance to and oversight of agencies' implementation of the act. OMB also has responsibility under the E-Government Act for developing PIA guidance and ensuring agency implementation of the PIA requirement. In July 1975, OMB issued guidance for implementing the provisions of the Privacy Act and has periodically issued additional guidance since then. OMB has also issued guidance on other data security and privacy-related issues including federal agency website privacy policies, interagency sharing of personal information, designation of senior staff responsible for privacy, data breach notification, and safeguarding personally identifiable information.

Technological Changes Have Made Key Elements of Privacy Laws Outdated

Technological developments since the Privacy Act became law in 1974 have radically changed the way information is organized and shared among organizations and individuals. Such advances have rendered some of the provisions of the Privacy Act and the E-Government Act of 2002 inadequate to fully protect all personally identifiable information collected, used, and maintained by the federal government.

For example, we reported in 2010 on privacy challenges associated with agencies using Web 2.0 technologies, such as web logs ("blogs"), social networking websites, video- and multimedia-sharing sites, and "wikis."² While the Privacy Act clearly applies to personal information maintained in systems owned and operated by the federal government, agencies often take advantage of commercial Web 2.0 offerings, in which case they have less control over the systems that maintain and exchange information, raising questions about whether personal information contained in those systems is protected under the act.

While OMB subsequently issued guidance to federal agencies for protecting privacy when using web-based technologies,³ we reported in June 2011 that agencies had made mixed progress in updating privacy policies and assessing privacy risks associated with their use of social media services, as required by OMB's guidance. A number of agencies had not updated their privacy policies or conducted PIAs relative to their use of third-party services such as Facebook and Twitter.⁴ Accordingly, we recommended that 8 agencies update their privacy policies and that 10 agencies conduct required PIAs. Most of the agencies agreed with our recommendations; however, 5 have not yet provided evidence that they have updated their privacy policies and 4 have not yet provided documentation that they have conducted PIAs.

²GAO, *Information Management: Challenges In Federal Agencies' Use of Web 2.0 Technologies*, GAO-10-872T (Washington, D.C.: July 22, 2010).

³Office of Management and Budget, Memorandum M-10-23: *Guidance for Agency Use of Third-Party Websites and Applications* (Washington, D.C.: June 25, 2010).

⁴GAO, *Social Media: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate*, GAO-11-605 (Washington, D.C.: June 28, 2011).

Another technology that has been increasingly used is data mining, which is used to discover information in massive databases, uncover hidden patterns, find subtle relationships in existing data, and predict future results. Data mining involves locating and retrieving information, including personally identifiable information, in complex ways.

In September 2011, we reported that the Department of Homeland Security (DHS) needed to improve executive oversight of systems supporting counterterrorism.⁵ We noted that DHS and three of its component agencies—U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and U.S. Citizenship and Immigration Services—had established policies that largely addressed the key elements and attributes needed to ensure that their data mining systems were effective and provided necessary privacy protections. However, we also noted, among other things, that DHS faced challenges in ensuring that all of its privacy-sensitive systems had timely and up-to-date PIAs. We recommended that that DHS develop requirements for providing additional scrutiny of privacy protections for sensitive information systems that are not transparent to the public through PIAs and investigate whether the information-sharing component of a certain data-mining system, the U.S. Immigration and Customs Enforcement Pattern Analysis and Information Collection program, should be deactivated until a PIA is approved that includes the component. DHS has taken action to address both of these recommendations.

Given the challenges in applying privacy laws and overseeing systems that contain personally identifiable information, the role of executives in federal departments and agencies charged with oversight of privacy issues is of critical importance. In 2008 we reported on agencies' designation of senior officials as focal points with overall responsibility for privacy.⁶ Among other things, we were asked to describe the organizational structures used by agencies to address privacy requirements and assess whether senior officials had oversight over key functions. Although federal laws and OMB guidance require agencies to designate a senior official for privacy with privacy oversight responsibilities, we found that the 12 agencies we reviewed had varying organizational structures to address privacy responsibilities and that

⁵GAO, *Data Mining: DHS Needs to Improve Executive Oversight of Systems Supporting Counterterrorism*, GAO-11-742 (Washington, D.C.: Sept. 7, 2011).

⁶GAO, *Privacy: Agencies Should Ensure That Designated Senior Officials Have Oversight of Key Functions*, GAO-08-603 (Washington, D.C.: May 30, 2008).

designated senior privacy officials did not always have oversight of all key privacy functions. Without such oversight, these officials may be unable to effectively serve as agency central focal points for information privacy. We recommended that six agencies take steps to ensure that their senior agency officials for privacy have oversight of all key privacy functions. Of the six agencies to which recommendations were made, four have provided evidence that they have fully addressed our recommendations.

Privacy Laws May Not Consistently Protect Personally Identifiable Information

In 2008, we issued a report on the sufficiency of privacy protections afforded by existing laws and guidance, in particular the Privacy Act, the E-Government Act, and related OMB guidance.⁷ Specifically, we found that while these laws and guidance set minimum requirements for agencies, they may not consistently protect personally identifiable information in all circumstances of its collection and use throughout the federal government and may not fully adhere to key privacy principles. We identified issues in three major areas:

Applying privacy protections consistently to all federal collection and use of personal information. The Privacy Act's definition of a system of records, which sets the scope of the act's protections, does not always apply whenever personal information is obtained and processed by federal agencies. For example, if agencies do not retrieve personal information by identifier, as may occur in data-mining systems, the act's protections do not apply. We previously reported that among the 25 agencies surveyed, the most frequently cited reason for collections of records not being considered Privacy Act systems of records was that the agency did not use a personal identifier to retrieve the information.⁸ Factors such as these have led experts to agree that the Privacy Act's system-of-records construct is too narrowly defined. An alternative for addressing these issues could include revising the system-of-records definition to cover all personally identifiable information collected, used, and maintained systematically by the federal government.

Ensuring that use of personally identifiable information is limited to a stated purpose. According to the purpose specification and use limitation principles, the use of personal information should be limited to a

⁷GAO, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, GAO-08-536 (Washington, D.C.: May 19, 2008).

⁸GAO, *Privacy Act: OMB Leadership Needed to Improve Agency Compliance*, GAO-03-304 (Washington, D.C.: June 30, 2003).

specified purpose. Yet current laws and guidance impose only modest requirements for describing the purposes for personal information and limiting how it is used. For example, agencies are not required to be specific in formulating purpose descriptions in their public notices. While purpose statements for certain law enforcement and antiterrorism systems might need to be phrased broadly enough so as not to reveal investigative techniques or the details of ongoing cases, very broadly defined purposes could allow for unnecessarily broad ranges of uses, thus calling into question whether meaningful limitations had been imposed. Examples for alternatives for addressing these issues include setting specific limits on the use of information within agencies and requiring agencies to establish formal agreements with external government entities before sharing personally identifiable information.

Establishing effective mechanisms for informing the public about privacy protections. According to the openness principle, the public should be informed about privacy policies and practices, and the accountability principle calls for those who control the collection or use of personal information to be held accountable for taking steps to ensure privacy protection. Public notices are a primary means for establishing accountability for privacy protections and giving individuals a measure of control over the use of their personal information. Yet concerns have been raised that Privacy Act notices may not serve this function well. Although the *Federal Register* is the government's official vehicle for issuing public notices, an expert panel convened for GAO questioned whether system-of-records notices published in the *Federal Register* effectively inform the public about government uses of personal information. Among others, options for addressing concerns about public notices could include setting requirements to ensure that purpose, collection, and use limitations are better addressed in the content of privacy notices and revising the Privacy Act to require that all notices be published on a standard website.

Updating the Privacy Act Can Provide Benefits

Addressing these three areas could provide a number of benefits. First, ensuring that privacy protections are applied consistently to all federal collection and use of information could help ensure that information not retrieved by identifier (such as may occur in data-mining applications, for example) is protected in the same way as information retrieved by identifier. Further, limiting the use of personally identifiable information to a stated purpose could help ensure a proper balance between allowing government agencies to collect and use such information and limiting that collection and use to what is necessary and relevant. Lastly, a clear and

effective notice can provide individuals with critical information about what personal data are to be collected, how they are to be used, and the circumstances under which they may be shared. An effective notice can also provide individuals with information they need to determine whether to provide their personal information (if voluntary), or who to contact to correct any errors that could result in an adverse determination about them.

We noted that some of these issues—such as those dealing with limitations on use and mechanisms for informing the public—could be addressed by OMB through revisions of or supplements to existing guidance. However, we further stressed that unilateral action by OMB would not have the benefit of public deliberations regarding how best to strike an appropriate balance between the government’s need to collect, process, and share personally identifiable information and the rights of individuals to know about such collections and be assured that they are only for limited purposes and uses.

Accordingly, we suggested that Congress consider amending applicable laws, such as the Privacy Act and E-Government Act, according to the alternatives we outlined, including

- revising the scope of the laws to cover all personally identifiable information collected, used, and maintained by the federal government;
- setting requirements to ensure that the collection and use of personally identifiable information is limited to a stated purpose; and
- establishing additional mechanisms for informing the public about privacy protections by revising requirements for the structure and publication of public notices.

In commenting on a draft of our report, OMB officials noted that they shared our concerns about privacy and listed guidance that the agency has issued in the areas of privacy and information security. The officials stated that they believed it would be important for Congress to consider potential amendments to the Privacy and E-Government Acts in the broader contexts of other privacy statutes and that it would be important for Congress to evaluate fully the potential impact of revisions.

In addition, in October 2011, you, the Chairman, introduced a bill to amend the Privacy Act. This bill—The Privacy Act Modernization for the Information Age Act of 2011—would, among other things, revise the Privacy Act to cover all personally identifiable information collected, used, and maintained by the federal government and ensure that collection and use of personally identifiable information is limited to a stated purpose.

However, revisions to the Privacy and E-Government Acts have not yet been enacted.

Agencies Can Take Action to Mitigate the Risks of Data Breaches, But Such Breaches Have Continued to Proliferate

In addition to relevant privacy laws and federal guidance, a key component of protecting citizens' personal information is ensuring the security of agencies' information systems and the information they contain by, among other things, preventing data breaches and reporting those breaches when they occur. In 2006, in the wake of a security breach at the Department of Veterans Affairs resulting in the compromise of personal data on millions of U.S. veterans, we testified on preventing and responding to improper disclosures of personal information in the federal government.⁹ We observed that agencies can take a number of actions to help guard against the possibility that databases of personally identifiable information are compromised. In particular, we noted two key steps agencies should take:

- Develop PIAs whenever information technology is used to process personal information. These assessments are a tool for agencies to fully consider the privacy implications of planned systems and data collections before implementation, when it may be easier to make critical adjustments.
- Ensure the implementation of a robust information security program as required by FISMA. Such a program includes periodic risk assessments; security awareness training; security policies, procedures, and practices, as well as tests of their effectiveness; and procedures for addressing deficiencies and for detecting, reporting, and responding to security incidents.

We also noted that data breaches could be prevented by limiting the collection of personal information, limiting the time such data are retained, limiting access to personal information and training personnel accordingly, and considering the use of technological controls such as encryption when data need to be stored on mobile devices.

OMB subsequently issued guidance that specifies minimum agency practices for using encryption to protect personally identifiable

⁹GAO, *Privacy: Preventing and Responding to Improper Disclosures of Personal Information*, GAO-06-833T (Washington, D.C.: June 8, 2006).

information. Memorandums M-06-15, *Safeguarding Personally Identifiable information*, and M-06-16, *Protection of Sensitive Agency Information*, reiterated existing agency responsibilities to protect personally identifiable information, and directed agencies to encrypt data on mobile computers and devices and follow National Institute of Standards and Technology (NIST) security guidelines regarding personally identifiable information that is accessed outside an agency's physical perimeter. In addition, OMB issued memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, which restated the M-06-16 recommendations as requirements and also required the use of NIST-certified cryptographic modules for encrypting sensitive information.

In 2008, we reported on the extent to which 24 major agencies had implemented encryption technologies.¹⁰ We found that agencies' implementation of encryption and development of plans to implement encryption of sensitive information varied, and that from July through September 2007, the agencies collectively reported that they had not yet installed encryption technology on about 70 percent of their laptop computers and handheld devices. Accordingly, we made recommendations to selected agencies to strengthen practices for planning and implementing the use of encryption. The agencies generally agreed with the recommendations and we have assessed that 6 of the 18 recommendations have been addressed.

Despite preventive measures, data breaches can still occur, and when they do it is critical that proper response policies and procedures be in place. We testified in 2006¹¹ that notification to individuals affected by data breaches and/or the public has clear benefits, such as allowing people to take steps to protect themselves from identity theft. Such notification is consistent with agencies' responsibility to inform individuals about how their information is being accessed and used, and it promotes accountability for privacy protection.

OMB issued guidance that updated and added requirements for reporting security breaches and the loss or unauthorized access of personally identifiable information. Specifically, OMB memorandum M-06-19 directs agencies to report all incidents involving personally identifiable

¹⁰GAO, *Information Security: Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains*, GAO-08-525 (Washington, D.C.: June 27, 2008).

¹¹GAO-06-833T.

information to US-CERT within 1 hour of discovery of the incident. In addition, OMB memorandum M-07-16 requires agencies to develop and implement breach notification policies governing how and under what circumstances affected parties are notified in the event of a data breach. Further, in a memorandum issued in September 2006, OMB recommended that agencies establish a core management group responsible for responding to the loss of personal information.

OMB also established requirements for reporting breaches within the government. In memorandum M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, OMB asked agencies to identify in their annual FISMA reports any physical or electronic incidents involving the loss of or unauthorized access to personally identifiable information. Agencies are also required to report numbers of incidents for the reporting period, the number of incidents the agency reported to US-CERT, and the number reported to law enforcement.

In 2007 we reported that while requiring agencies to notify affected consumers of a data breach may encourage better security practices and help mitigate potential harm, it also presents certain costs and challenges.¹² Federal banking regulators and the President's Identity Theft Task Force had advocated a notification standard—the conditions requiring notification—that was risk based, allowing individuals to take appropriate measures where the risk of harm existed, while ensuring they are only notified in cases where the level of risk warrants such action. Use of such a risk-based standard could avoid undue burden on organizations and unnecessary and counterproductive notifications to consumers about breaches that present little risk.

Data Breaches Continue to Proliferate in the Public and Private Sectors

Over the last several years, we have continued to report that federal agency systems are vulnerable to cyber attacks and the potential compromise of sensitive information, including personally identifiable information.¹³ For fiscal year 2011, agency inspector general and GAO assessments of information security controls revealed that most major

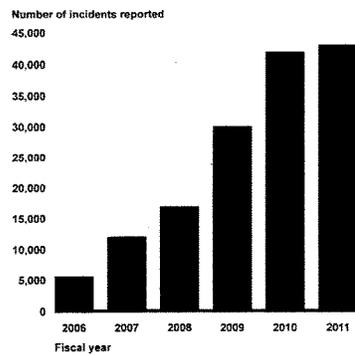
¹²GAO, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent is Unknown*, GAO-07-737 (Washington, D.C.: June 4, 2007).

¹³GAO, *Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements*, GAO-12-137 (Washington, D.C.: Oct. 3, 2011).

federal agencies had weaknesses in most of five major categories of information system controls. Further, over the past several years, we and agency inspectors general have made hundreds of recommendations to resolve similar previously identified significant control deficiencies. We have also recommended that agencies fully implement comprehensive, agency-wide information security programs as required by FISMA, including by correcting weaknesses in specific areas of their programs. The effective implementation of these recommendations will strengthen the security posture at these agencies, which will in turn help ensure the protection of personally identifiable information they collect and use.

Federal agencies have also reported increasing numbers of security incidents that placed sensitive information at risk, with potentially serious impacts on federal operations, assets, and people. Over the past 6 years, the number of incidents reported by federal agencies to US-CERT has increased from 5,503 incidents in fiscal year 2006 to 42,887 incidents in fiscal year 2011, an increase of nearly 680 percent. (See fig. 1.) Of the incidents occurring in 2011, 15,560 involved unauthorized disclosure of personally identifiable information, a 19 percent increase over the 13,017 personally identifiable information incidents that occurred in 2010.

Figure 1: Incidents Reported to US-CERT: Fiscal Years 2006 - 2011



Source: GAO analysis of US-CERT data for fiscal years 2006-2011.

Reported attacks and unintentional incidents involving federal, private and

critical infrastructure systems involve a wide range of incidents including data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices. The following examples from news media and other public sources illustrate some of the risks:

- In May 2012, the Federal Retirement Thrift Investment Board reported a sophisticated cyber attack on a computer belonging to a third party, which provided services to the Thrift Savings Plan. As a result of the attack, 123,000 participants had their personal information accessed. According to the board, the information accessed included 46,587 individuals' names, addresses, and Social Security numbers, and 79,614 individuals' Social Security numbers and other Thrift Savings Plan-related information.
- In April 2012, hackers breached a server at the Utah Department of Health to access thousands of Medicaid records. Included in the breach were Medicaid recipients and clients of the Children's Health Insurance Plan. About 280,000 people had their Social Security numbers exposed. In addition, another 350,000 people listed in the eligibility inquiries may have had other sensitive data stolen, including names, birth dates, and addresses.
- In March 2012, a news wire service reported that the senior commander of the North Atlantic Treaty Organization (NATO) had been the target of repeated cyber attacks using Facebook that were believed to have originated in China. According to the article, hackers repeatedly tried to dupe those close to the commander by setting up fake Facebook accounts in his name in the hope that his acquaintances would make contact and answer private messages, potentially divulging sensitive information about the commander or themselves.
- In March 2012, it was reported that Blue Cross Blue Shield of Tennessee paid out a settlement of \$1.5 million to the U.S. Department of Health and Human Services arising from potential violations stemming from the theft of 57 unencrypted computer hard drives that contained protected health information of over 1 million individuals.

Incidents such as these illustrate that sensitive personally identifiable information remains at risk and that improved protections are needed to ensure the privacy of information collected by the government. While OMB has taken steps through the guidance I described to set requirements for agencies to follow, it is unclear the extent to which all agencies, including smaller agencies such as the Federal Retirement

Thirst Investment Board, are adhering to OMB's guidelines.

In summary, ensuring the privacy and security of personal information collected by the federal government remains a challenge, particularly in light of the increasing dependence on networked information systems that can store, process, and transfer vast amounts of data. These challenges include updating federal laws and guidance to reflect current practices for collecting and using information while striking an appropriate balance between privacy concerns and the government's need to collect information from individuals. They also involve implementing sound practices for securing and applying privacy protection principles to federal systems and the information they contain. Without sufficient attention to these matters, Americans' personally identifiable information remains at risk.

Chairman Akaka, Ranking Member Johnson, and members of the Subcommittee, this concludes my statement. I would be happy to answer any questions you have at this time.

Contact and Acknowledgments

If you have any questions regarding this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Other key contributors to this statement include John de Ferrari, Assistant Director; Melina Asencio; Sher'rie Bacon; Anjalique Lawrence; Kathleen Lovett Epperson; Lee McCracken; David Plocher; and Jeffrey Woodward.

Senate Committee on Homeland Security and Governmental Affairs

**Senate Subcommittee on Oversight of Government Management,
the Federal Workforce, and the District of Columbia**

**Hearing: "State of Federal Privacy and Data Security Law:
Lagging Behind the Times?"**

**Peter Swire
C. William O'Neill Professor of Law
Moritz College of Law
The Ohio State University**

July 31, 2012

Chairman Akaka, Ranking Member Johnson, and distinguished members of the Committee, thank you for inviting me to testify on "State of Federal Privacy and Data Security Law: Lagging Behind the Times?"

I am the C. William O'Neill Professor of Law at the Moritz College of Law of the Ohio State University. In 1999 I was named Chief Counselor for Privacy, in the U.S. Office of Management and Budget. In that role, I was the first (and thus far the only) person to have government-wide responsibility for privacy policy. As Chief Counselor for Privacy, I worked extensively with the Privacy Act of 1974, helped institutionalize the practice of Privacy Impact Assessments for federal systems, and addressed many other privacy and cybersecurity issues affecting federal agencies. Since then, I have continued to write and speak extensively on privacy and security issues.

For this testimony, Committee Staff requested that I address a range of issues concerning federal agency privacy and data practices. As the other testimony for this hearing demonstrates, there are many different privacy-related challenges facing federal agencies today. My testimony addresses four topics, with the key points set forth in the introduction:

- 1) **The Senate Should Promptly Confirm the Five Nominees for the Privacy and Civil Liberties Oversight Board.** The most important short-term action the Senate can take on privacy is to confirm the five nominees for the PCLOB, as voted out of the Judiciary Committee. All five nominees are supported by 9/11 Commission Co-Chairs Tom Kean and Lee Hamilton. Although there were

dissenting votes in committee concerning the proposed Chairman, David Medine, he is an outstanding and experienced nominee. By statute, only the Chairman can hire staff, and the Senate should act promptly to put the Board into operation.

- 2) **Congress should create a federal Chief Privacy Officer by statute, to improve coordination of privacy policy across federal agencies.** A federal CPO would notably improve the clearance process within the executive branch for privacy policy, as well as help coordinate the many trans-border privacy issues that arise in our world of pervasively global data flows. Without statutory support, existing agencies may stymie creation of that position. I suggest that the federal CPO might take the lead for non-classified federal information technology systems, while the PCLOB could take the lead for classified systems.
- 3) **There is an important loophole in the Privacy Act, but the problem can best be addressed by changes to the E-Government Act.** The proposed S. 1732 to update the Privacy Act correctly recognizes that the definition of “system of records” has an important loophole. The current definition applies only to records “retrieved by name,” and modern search engines often identify records even when the name does not appear in the search term.
 - a) The proposed amendment would close the loophole, but have the effect of requiring a far larger number of systems of records notices by federal agencies. In my view, this increase would create compliance burdens but not lead to significant privacy improvements.
 - b) I believe a more promising approach would be to improve Privacy Impact Assessments under the E-Government Act of 2002. For instance, OMB or an inter-agency council should post agency PIAs to a unified web site, so that the public can compare agency PIAs. Agencies should likely have a mechanism where public comments would be posted for PIAs. In addition, agencies could be required to respond to these public comments.
- 4) **The oversight process should focus more attention on the line between identified and de-identified data in federal agencies.** Specifically, the Federal Trade Commission has proposed a promising approach for defining de-identified data when held in the private sector. An important question is how that approach might be modified for use in federal agencies.

In summary, this Committee is performing an important service by focusing attention on the privacy practices of federal agencies. I hope that the comments here will be of use to the Committee in its oversight and legislative efforts.

I. The Senate Promptly Should Confirm the Five Nominees for the Privacy and Civil Liberties Oversight Board

Before turning to the long-term issues of privacy and the federal government, there is one pressing privacy item for action by the Senate as soon as possible. The Senate should confirm the five nominees for the Privacy and Civil Liberties Oversight Board, as voted out of the Judiciary Committee. Last week’s Senate vote on the cybersecurity bill makes confirmation even more urgent.

Currently, the PCLOB is not in operation. The 9/11 Commission recommended implementing this type of Board to increase oversight of the expanded information sharing practices among agencies adopted after the attacks of September 11, 2001. The Senate confirmed members of the PCLOB in 2006, and the Board began operation. Controversy emerged about the original Board's lack of independence. As a result, a revised structure for the Board was established in 2007, as part of the Implementing Recommendations of the 9/11 Commission Act. The revised structure creates staggered 6-year terms for each of the five Members, and required the Chairman to work full-time for the Board.

No members of the Board have been confirmed since that time. The Senate Judiciary Committee voted and approved all five nominees this May, but no date has been scheduled for floor action. Having a functioning Privacy and Civil Liberties Oversight Board is important under any circumstances, to ensure regular and effective examination of the information sharing and privacy practices for homeland security and other anti-terrorism activities.

The importance of implementing the Board becomes even greater, however, due to the expanded information sharing in the proposed cybersecurity legislation. A key purpose behind that legislation is to enhance information sharing as a tool for fighting cyber-attacks. A key safeguard is for the Board to scrutinize this type of information sharing. In my view, putting the Board in place should be a required component of approving cybersecurity legislation.

The full slate of nominees has received a strong letter of support from the Bipartisan Policy Center, signed by Tom Kean, former Republican Governor of New Jersey, and Lee Hamilton, former Democratic Congressman from Indiana.¹ Governor Kean and Rep. Hamilton co-chaired the 9/11 Commission. In their letter this June, the authors wrote: "The Board is designed to play a crucial oversight role in preventing the intentional or accidental misuse of personal information across the government, and its establishment should be a high priority." They thus wrote to "advocate for the confirmation of the five nominees" to the Board, all of whom have been reported out of committee.

I would also like to comment specifically in support of the nomination of David Medine to serve as the Chairman of the Privacy and Civil Liberties Board. Mr. Medine received dissenting votes on his nomination in committee, although there are no public reports of any basis for opposition or concern. I have known Mr. Medine professionally for over 15 years. From 1992 to 2000, Mr. Medine was the senior civil servant expert on privacy at the Federal Trade Commission, serving as the Associate Director for Financial Practices. Shortly after, he became a partner at the leading law firm WilmerHale, where he worked with private-sector clients primarily on privacy and data security. In the latter position, he counseled clients on how to comply with complex privacy requirements. I believe this real-world compliance experience is highly relevant to realistic privacy protection. Mr. Medine

has experience both in enforcing to protect privacy and in the burdens that exist when privacy rules are overly strict or badly drafted. This balanced experience makes him an outstanding person to Chair the Privacy and Civil Liberties Oversight Board.

The statute creating the Board requires the Chairman to work full time. In addition, the statute allows only the Chairman to hire staff: "The chairman of the Board ... shall appoint and fix the compensation of a full-time executive director and such other personnel as may be necessary to enable the Board to carry out its functions." Clearly, the Board cannot carry out its work as the statute intends if there is no Chairman in place. The Senate should act promptly to confirm all five nominees.

II. The Importance of Coordinating Federal Privacy Policy

The Committee asked me to write about my experience as Chief Counselor for Privacy, including the merits of having a federal Chief Privacy Officer to coordinate and oversee privacy policy across the federal government. I support the proposal by Senator Akaka in S. 1732 to create such an office. The discussion here explains some key reasons that support creating such a position. It then suggests how to structure such an office, with the federal CPO taking the lead on non-classified federal information systems, and the PCLOB taking the lead on classified systems.

Why the Federal Government Should Have a Privacy Policy Office

In a piece prepared for publication in the Stanford Law Review in 2000 (but not ultimately published), I explained the role that the Chief Counselor for Privacy played during the intense privacy policy debates of the late 1990's.ⁱⁱ Earlier this year I returned to the subject in a law review article on "Why the Federal Government Should Have a Privacy Policy Office."ⁱⁱⁱ That article highlights the role such a privacy policy office would play in the inter-agency clearance process and in coordinating a unified approach to the large number of international privacy issues.

First, the CPO is important for the "clearance" process.^{iv} To ensure a unified administration position, for congressional testimony, executive orders, and many other documents, drafts are circulated for clearance among the various agencies and components of the Executive Office of the President. Once comments are received, discussions are sometimes needed to resolve differences of opinion, with appeal to more senior officials if differences are not resolved at lower levels. In addition to these structured clearance procedures, agency experts on an issue such as privacy often get engaged earlier in the policy planning process, in a variety of working groups and less-formal methods of sharing expertise and views.

From my time as Chief Counselor for Privacy, the number of privacy issues addressed by federal agencies is far greater than many people realize. Here is a list of the sorts of privacy issues that can arise in each of the cabinet departments:

- Department of Agriculture: Migrant worker records.
- Departments of Defense and Veterans Affairs: Records of service members.
- Department of Education: Education records, including for for-profit institutions.
- Department of Energy: Smart grid.
- Department of Health and Human Services: Medical records; many forms of human services records.
- Department of Homeland Security: Numerous issues, including transportation safety and immigration.
- Department of Housing and Urban Development: Public housing records.
- Department of Interior: National park reservations and other services provided online.
- Department of Justice: Numerous issues.
- Department of Labor: Records of union membership.
- Department of State: International privacy issues.
- Department of Transportation: Drone surveillance.
- Department of Treasury: Financial privacy; money laundering.

This list shows a wide variety of privacy issues, and also that privacy issues emerge for new agencies over time. As one example, surveillance by drones is becoming an important privacy issue as the Federal Aviation Administration permits expanded use of drones within the borders of the United States. For these kinds of emerging issues, I believe the expertise developed by a federal CPO would be quite useful.

Second, along with clearance, the executive branch needs effective coordination to develop and announce the administration position in international settings. Data flows today are pervasively global. We are reminded of this reality by the ongoing debates about the European Union's draft Regulation on Data Protection. A very wide range of Internet and other private-sector data practices would be affected if that Regulation were to go into effect as currently written. For the public sector, there are also many cross-border issues, such as for passenger name records, law enforcement investigations, and many others. One of my current research projects analyzes how cloud computing, together with the widespread adoption of encryption, is making international cooperation on law enforcement investigations much more important than in the past.^v For the federal government, the increasing number and complexity of trans-border privacy issues means that coordination of privacy policy would be very helpful.

From my time at OMB and in the National Economic Council, there are certainly existing mechanisms for policy coordination. The NEC and National Security Council are experienced at bringing together the relevant agencies to coordinate on complex policy problems. I believe these policy mechanisms, however, are not a good match for the ongoing privacy challenges. Resolving privacy issues often requires cross-cutting expertise, drawing on domains including information technology, law, business practices, and policy. When this complexity is added to the complex inter-agency and international dimensions of the issue, the policy councils do not have the staffing and infrastructure to do a good enough job on managing privacy issues over time.

How to Structure Federal Privacy Policy Leadership

I believe that Congress should create by legislation the office of the federal Chief Privacy Officer, and similarly require each major agency to have a CPO.

The administration's recent Green Paper and White Paper on commercial privacy protection suggest the role that legislation can play here. The Green Paper in 2011 contained the idea of having an office in the Department of Commerce to coordinate privacy policy for commercial actors.^{vi} That office was dropped from the 2012 White Paper.^{vii} My sense is that this shift reflects the institutional difficulties in establishing a new office unless there is Congressional support. Existing offices are reluctant to cede their current roles and budget. Congress mandated creation of the office of the Chief Privacy Officer when it created the Department of Homeland Security, and the Chief Privacy Officer in that department has been effective at having institutional support compared with other agencies.

Based on my experience, I believe that OMB is an effective location for the federal CPO. This fits the management responsibilities of the Office of Management and Budget. In 1999, after a survey found that privacy policies were lacking on many federal agency websites, we were tasked with defining acceptable privacy policies and then making sure that agencies posted them. That experience taught my staff and me the challenges of complying with rules and public scrutiny. That kind of experience helps the CPO be more realistic when developing policy that other organizations are expected to follow.

One topic that could benefit from further discussion is how to integrate a federal CPO with the PCLOB. I suggest some ideas here, but other approaches are worth considering. **One way to split responsibilities is for the federal CPO to coordinate policy and oversight for unclassified information technology systems, while the PCLOB would take the lead on classified systems.** This apportionment of responsibilities would parallel the existing, different requirements for classified and unclassified systems generally. **In terms of function, the federal CPO would take the lead on clearance and other issues of cross-agency coordination.** The PCLOB is designed to be independent of the executive branch, and thus would not play that inter-agency coordination role.

Instead, its principal responsibilities would include oversight and investigation of data used in connection with anti-terrorism efforts.

III. There is an Important Loophole in the Privacy Act, but the Problem Can Best Be Addressed by Changes to the E-Government Act

I now turn to the topic of amending the Privacy Act of 1974 and related statutes that create the framework for privacy protection in federal agencies. Chairman Akaka has taken a leadership position in proposing ways to update the Privacy Act for our modern information environment, including in S. 1732, the Privacy Act Modernization for the Information Age Act of 2011. As just discussed, I support that bill's approach to reconfiguring the management and coordination of privacy actions of federal agencies. I believe that a somewhat different approach may be more constructive, however, when it comes to amendments to the core definitions in the Privacy Act.

This portion of the testimony first provides a brief background about the Privacy Act of 1974. It next analyzes the "retrieved by name" loophole that S. 1732 seeks to close, before explaining why amendments to the E-Government Act of 2002 may be a more effective way to protect privacy while managing compliance costs of federal agencies.

Background on the Privacy Act of 1974

The Privacy Act was passed at the end of 1974, the year that President Nixon resigned from office. Along with the Freedom of Information Act, it was enacted to address a pattern of secret government surveillance of American citizens. The history of this surveillance has been told before, but it is useful to periodically remind ourselves about actions such as the years of wiretapping of Martin Luther King, Jr., the domestic intelligence files created by the FBI on hundreds of thousands of Americans, and the use of IRS tax records against the President's political "enemies list."^{viii} We should learn from this history so we do not repeat it.

The Privacy Act as enacted was based on a 1973 report from the Department of Health, Education, and Welfare, which proposed five principles for a Code of Fair Information Practices:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.

5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

As enacted, the Privacy Act essentially codified these principles. Individuals start with a baseline right that their personal information can only be disclosed with their consent. An important aspect of the law was to publish “system of records notices” (SORNs) in the Federal Register, so that the general public could learn about the existence and nature of federal databases. These SORNs provide details such as categories of records maintained, ways for individuals to access their own records, and routine uses that permit additional disclosures by the agency without individual consent.^{ix}

During my time at OMB, I was the official responsible for answering questions about interpreting the Privacy Act, working closely with the Department of Justice office that publishes collections of Privacy Act cases. Based on my experience, the Privacy Act today continues to play a vital role in structuring federal agencies’ use of personal information. The privacy-related actions of federal agencies today are far better than they would be without the Privacy Act. SORNs help agencies consider what uses of information are lawful and appropriate, especially where the SORNs are thoughtfully crafted and not boilerplate. In my experience, agency Privacy Act officers thoughtfully apply the law’s Fair Information Practices to individual disputes and situations as they arise.

The “Retrieved by Name” Loophole in the Privacy Act

The core definitions of the Privacy Act today are the same as when the law was enacted 38 years ago. Our information processing technology today is comprehensively different than in 1974, and so the Committee is justifiably exploring whether key definitions should be updated. S. 1732 addresses the most glaring weakness in the existing definitions, which can be called the “retrieved by name” loophole. My view, however, is that there may be more effective ways to address that problem, notably through changes to the E-Government Act of 2002.

The definition of “system of records” is central to Privacy Act because it is the main device for dividing what is covered by Privacy Act requirements and what is not. In any regulatory system, the definition of the scope of coverage is especially important – if something is outside the scope of a law, then agencies or other regulated entities do not have to worry about the other details of compliance.

Since 1974, the Privacy Act has defined “systems of records” to mean “a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.” (emphasis added) For each system of records, the agency must publish a system of records notice (“SORN”) in the Federal Register.^x

The main problem with the definition of systems of records is that it applies only when “information is retrieved by the name of the individual.” This approach made sense in the days when records were kept primarily in a physical file drawer. If you wanted to access a record, you would thumb through the alphabetical list of file folders until you found the right person. This approach also made a certain amount of sense in the early world of mainframe computers. The IRS, for instance, would organize tax records by name or Social Security number. That type of highly structured system of records is covered by the Privacy Act, because the records are retrieved by name or the person’s identifying number.

This definition, however, fails to cover many other ways that agencies handle personal information today. The 1977 Privacy Protection Study Commission gave the example of a search by the Veterans Administration by psychiatric diagnosis. Because the search was by diagnosis, and not by name, the Privacy Act simply did not apply.^{xi} In essence, the Privacy Act definition applies to structured record sets listed by name, but not to other ways agencies can use records to identify and then act on individuals.

Due to increased speed and capacity of computer search and data mining over the years, this gap in the Privacy Act’s coverage has widened significantly. Because search is a daily part of our lives today, sometimes it is hard to remember that Google was not incorporated until 1998. Individuals and federal agencies today complete an enormous number of searches without use of a name, but people’s names still pop up in the results. Data mining takes that concept even further – federal agencies sift through innumerable records in order to spot patterns and turn up suspects or individuals that are of interest for one reason or another. But the Privacy Act simply does not apply to the vast bulk of records where there is no organized retrieval by name or number.

To address this gap, S. 1732 would broaden the definition of “system of records” to include “a group of any records maintained by, or otherwise under the control of any agency that is used for any authorized purpose by or on behalf of the agency.” The proposed amendment recognizes how records are actually retrieved today, often without explicitly searching by name or identifying number. The proposed amendment would close the loophole that has been recognized since the 1970s.^{xii}

Under the new approach, the key trigger for Privacy Act coverage would be what qualifies as a “record.” The definition of “record” focuses on each individual, rather than how records are grouped in an agency’s filing system. Under the Privacy Act, the term “record” applies broadly to “any item, collection, or grouping of information about an individual that is maintained by an agency.” The Act provides examples of what count as “records,” such as “his education, financial transactions, medical history, and criminal or employment history.” Finally, a record “contains

his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.”

The proposed amendment would close the “retrieved by name” loophole but would quite possibly also lead to an enormous increase in the number of system of records notices. S. 1732 would apply to a “group of any records” under the control of an agency. My concern is that there would be too many “groups of any records.” Records today are gathered and used for many purposes. Under the proposed revisions to the Privacy Act, agencies would have to go through the bureaucratic requirements of SORNs for each of those groups. SORNs provide important functions such as providing public notice and ensuring that the full set of Privacy Act fair information practices apply. The Information Security and Privacy Advisory Board’s 2009 report on federal privacy protection, however, found that SORNs “are difficult to understand, overly vague and general, and reach only a narrow audience.”^{xiii} I believe the Congress should consider other alternatives before acting to increase the number of SORNs in this way.

Consider Improving Privacy Impact Assessments Rather than Directly Amending the Privacy Act Loophole

The discussion of the “retrieved by name” loophole shows an important flaw in the Privacy Act’s goals of providing notice about agency privacy practices and ensuring consideration of privacy risks. Rather than amending the Privacy Act, however, I think that better progress can likely be made by improving the E-Government Act of 2002.

The E-Gov Act requires agencies to issue Privacy Impact Assessments in connection with the “development or procurement of new information technology.” Section 208 of the E-Gov Act requires PIAs to be commensurate with the size of the information system, the sensitivity of the identifiable information, and the risk of harm from unauthorized release.

In considering the vast range of data used by federal agencies, my sense is that that the trigger for requiring a PIA is more practical than the proposed trigger for requiring a SORN. A Privacy Impact Assessment is required when developing or procuring a new information technology system. In this way, the PIA is built into an ongoing process, such as a procurement. Ideally, the PIA is completed early enough in the process to identify privacy risks, leading to a more effective and less privacy-intrusive system. In addition, OMB has issued Guidance under the E-Gov Act that contains common-sense exceptions to the requirement that an agency do a PIA, such as for minor changes to a system that do not create new privacy risks.^{xiv}

By contrast, the proposed amendment would trigger a Systems of Record Notice for “a group of any records” controlled by the agency. My concern is that the number of SORNs would need to climb substantially to cover this apparently very broad language. OMB has authority under the E-Gov Act to create pragmatic

exceptions to when a PIA is required, but it is not clear to me that OMB has similar such authority under the Privacy Act. In addition, the Privacy Act does not have the risk-based approach of the E-Gov Act, where the level of privacy work by the agency is supposed to be commensurate with the privacy risks.

My related concern is that increasing the number of SORNs would not actually improve privacy protection. At least ideally, the goal of a Privacy Impact Assessment is to do a nuanced examination of the privacy risks in a new procurement or computer system. This sort of nuanced examination, however, is unlikely to occur if an agency has to slog through a huge number of routine Privacy Act SORNs. If the number of SORNs climbs sharply, I fear that agencies will adopt too much of a “check the box” approach to privacy protection, simply filing Privacy Act notices that are uninformative and do not adequately address actual privacy risks.

In 2003, OMB issued Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.^{xv} This Guidance does a straightforward and reasonable job of implementing the E-Gov Act as written. I have concerns, however, about how well the Guidance has been implemented over time.

Going forward, this Subcommittee and Committee may find it useful to conduct oversight specifically on implementation for Privacy Impact Assessments of the E-Gov Act and the OMB guidance. My sense of implementation of PIAs is similar to that found by the ISPAB. The Department of Homeland Security has done a notably good job in preparing and publishing PIAs, in no small part due to the visible leadership and responsibilities of the Department’s Chief Privacy Officers, including Mary Ellen Callahan who is testifying in this hearing today. Other agencies, however, have done a more superficial job in drafting their PIAs. I am not aware of any major, visible discussion about how to bring the quality of those other agencies up to the quality at DHS.

I have two suggestions for improvement to the privacy parts of the E-Gov Act. The first concerns making it easier to find and compare agency PIAs. The Act directs agencies to submit their PIAs to OMB. They are also directed to make their PIAs publicly available, with certain exceptions for national security and other exceptions. Notably, these two requirements do not seem to be currently linked – I can find no easy way to find the PIAs of different agencies in order to compare them. **I think it would likely improve the quality and consistency of PIAs if OMB or one of the inter-agency councils created a process for posting agency PIAs to a unified site that is publicly available.**

Second, the E-Gov Act could have more effective methods for public comment and input. As a first step, **agencies should likely have a mechanism where public comments would get posted for PIAs. In addition, agencies could be required to respond to comments.** The idea here is not to create full Administrative Procedure Act notice-and-comment, where a rulemaking cannot go forward until

the comments are complete. Instead, my suggestion is a lighter touch approach, where the agency would publish the public comments and give some response. This sort of “nudge” to an agency is consistent with the light-touch or “nudge” approach to regulation that Office of Information and Regulatory Affairs Director Cass Sunstein has brought to OMB.

IV. The Oversight Process Should Focus More Attention on the Line between Identified and De-Identified Data in Federal Agencies

One increasingly important issue over time is determining how to draw the line between data that is identified or not. Privacy requirements apply where the links to a specific person are clear enough. By contrast, those requirements do not apply where the links are not clear enough, such as where enough details are removed so that the information can be considered de-identified. The issue of de-identification has begun to receive significantly more attention in connection with personal privacy, as reflected this year in the administration’s White Paper and the FTC’s privacy report. **My discussion here suggests that the oversight process should focus more attention on the line between identified and de-identified data in federal agencies. Specifically, the Federal Trade Commission has proposed a promising approach for defining de-identified data when held in the private sector. An important question is how that approach might be modified for use in federal agencies.**

This spring the administration released its White Paper on “A Framework for Protecting Privacy and Promoting Innovation.” The White Paper applies to personal data held in the private sector. The title reflects the risks to individuals if privacy is not protected effectively. It also reflects the importance of creating good information rules in order to foster innovation and growth in our information economy.

The issue of de-identified data creates a vital opportunity to meet both goals—protect privacy while using data for innovation, growth, and the other goals of the private and public sectors. At least in theory, de-identified data allows us to have our cake and eat it, too. With de-identified data, we strip out the name and other information that reveals identity, but we nonetheless can process the data, do research, discover patterns, and innovate in how we respond to the information.

In recent years, we have learned a great deal about when and how it is possible to “re-identify” data—to link a person’s name with supposedly de-identified data. Two big trends have made it harder to keep information de-identified. First, search on the Web has gotten much better. Today’s search engines let anyone link together tidbits from previously hard-to-link data sources. Second, the amount of information on the Web about a typical person has grown astronomically, including all of the personal details on a person’s blog or Facebook page.

The combination of efficient search tools and lots of data means that there is a higher likelihood today that a person's records can be re-identified even if the name and other traditional identifiers are deleted. For instance, a de-identified medical record might state that a person in Ohio had minor hand surgery on April 3. In the past, it would have been difficult or impossible for an outsider to figure out the name. Today, online search might turn up a social network thread about the hand surgery—there are multiple such surgeries in Ohio each day, but not that many. A bit of follow-up research, using the rest of the supposedly de-identified information, might easily pinpoint the person who had the surgery.

As experts have analyzed these facts about re-identification, some have concluded that the entire effort to de-identify data has failed, because of the risk of linking information back to the individual.^{xvi} Others have emphasized the limited actual success of re-identification efforts in practice, and found that the benefits such as research and innovation are so great that they outweigh the privacy risks.^{xvii}

In response to public comments on the issue of de-identification, the FTC in its privacy report this spring proposed a promising approach for treating data as de-identified. The FTC provides what amounts to a safe harbor where: "(1) a given data set is not reasonably identifiable; (2) the company publicly commits not to re-identify it, and (3) the company requires any downstream users of the data to keep it in de-identified form." A key part of the approach is that the entity holding the data promises not to re-identify it. For instance, even if the entity could theoretically investigate who had the hand surgery on April 3, it won't do the investigation, and the data can be properly treated as de-identified.

I believe a similar approach could help federal agencies gain benefits from using data while holding it in de-identified form. The precise FTC approach will not work, however. Enforcement of the FTC approach is based on the company's public commitment not to re-identify the data. A violation of that commitment is enforceable under Section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive trade practices. That Act applies only to commercial actors, and not federal agencies.

The question is how to take this approach of promising not to re-identify, and applying it to federal agencies. This is a novel question, and I do not know today how best to translate the FTC approach to federal agencies. I believe it is a worthwhile endeavor, however, because such an approach could open agencies to more of the modern benefits of using data while also protecting privacy and reducing compliance costs with privacy requirements. Federal agencies also face the issue that information might be re-identified in some instances for law enforcement, national security, or related purposes. To address this possibility, one might require agencies to notify the PCLOB (assuming it is up and running) if they re-identify data for national security or related reasons.

In conclusion on de-identification, the ability to de-identify is becoming more technically challenging while the need for effective de-identification is increasing. The FTC has proposed an approach that combines promises not to re-identify with the available technical measures. This fall I will be conducting a project on de-identification with the Future of Privacy Forum, seeking to identify and improve best practices in the area.^{xviii} Along with efforts in the private sector, this Committee in its oversight role can encourage OMB and federal agencies to create guidance and best practices for de-identification in the public sector.

V. Conclusion

In conclusion, I commend the Committee for its attention to these important issues of privacy protection and federal agencies. Thank you for the opportunity to testify, and I welcome any questions you may have.

ⁱ <http://www.scribd.com/doc/98470241/Letter-to-Senate-Majority-Leader-Harry-Reid-and-Senate-Minority-Leader-Mitch-McConnell-from-BPC-Homeland-Security-Project-Co-Chairs-Lee-Hamilton-and-T>

ⁱⁱ Peter P. Swire, *The Administration Response to the Challenges of Protecting Privacy*, Stanford Law Review Symposium on Privacy, 2000, available at <http://www.peterswire.net/pspublications-unpub.htm>.

ⁱⁱⁱ Peter Swire, *Why the Federal Government Should Have a Privacy Policy Office*, 10 J. Telecommunications & High Technology Law 41 (2012), available at <http://ssrn.com/abstract=1960634>.

^{iv} I discussed the clearance process in some detail in the 2000 document.

^v Peter P. Swire, *From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud*, available at <http://ssrn.com/abstract=2038871>.

^{vi} U.S. Department of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, 2010, available at <http://www.commerce.gov/node/12471>.

^{vii} The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, 2012, available at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

^{viii} For one discussion of the history, see Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 George Washington L. Rev. 1304 (2004), available at <http://ssrn.com/abstract=586616>.

^{ix} 5 U.S.C. §552a(e)(4).

^x 5 U.S.C. §552a(e)(4).

^{xi} PRIVACY PROT. STUDY COMM'N, THE PRIVACY ACT OF 1974: AN ASSESSMENT 6-7 (1974), available at <http://epic.org/privacy/ppsc1977report/appendix4.html> (providing an example of a Veterans' Administration search by psychiatric diagnosis)

that was not covered by the Act). For in-depth discussion of the definitions that trigger privacy requirements, see Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally identifiable Information*, 86 New York University Law Review 1814 (2011).

^{xiii} The approach in S. 1732 is similar to the approach in the work of the Center for Democracy and Technology on how to update the Privacy Act. CDT would delete the current definition of “system of records,” thus expanding the scope of the Privacy Act to the broader range of agency actions affecting “records.” See eprivacyact.org (showing draft legislation favored by CDT).

^{xiii} Information Security and Privacy Advisory Board, *Toward a 21st Century Framework for Federal Government Privacy Policy*, May 2009, available at <http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/ispab-report-may2009.pdf>.

^{xiv} M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, available at http://www.whitehouse.gov/omb/memoranda_m03-22/.

^{xv} M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, available at http://www.whitehouse.gov/omb/memoranda_m03-22/.

^{xvi} Paul Ohm, “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization” *UCLA Law Review* 57 (1701) (2010), available at <http://ssrn.com/abstract=1450006>.

^{xvii} Jane Yakowitz, “Tragedy of the Data Commons,” *Harvard Journal of Law and Technology* 25 (2011), available at <http://ssrn.com/abstract=1789749>.

^{xviii} The comments on de-identification here draw in part on material that I submitted to the Department of Commerce in its request for comments on the privacy multistakeholder process. See <http://www.ntia.doc.gov/federal-register-notice/2012/comments-multistakeholder-process>. See also Peter Swire, “Keynote – Setting the State: How De-Identification Came into U.S. Law and Why the Debate Matters Today,” *Future of Privacy Forum*, Conference on De-Identification, 2011, available at <http://www.peterswire.net/psspeeches2011.htm>.



Statement of Christopher R. Calabrese, Legislative Counsel

American Civil Liberties Union
Washington Legislative Office

On

State Of Federal Privacy and Data Security Law: Lagging Behind the Times?

Before the Senate Committee on Homeland Security and Governmental Affairs
Subcommittee on Oversight of Government Management, the Federal Workforce,
and the District of Columbia

July 31, 2012

Good morning Chairman Akaka, Ranking Member Johnson, and Members of the Committee. Thank you for the opportunity to testify on behalf of the American Civil Liberties Union (ACLU) its more than half a million members, countless additional activists and supporters, and fifty-three affiliates nationwide, about the importance of updating the Privacy Act and assuring accountability and oversight regarding how the federal government handles personal information.

I. Introduction

The Privacy Act of 1974 was a landmark statute that has provided significant privacy protections but now needs to be updated. The Act formed the foundation for information privacy law, not just in the United States but around the world. The principles it delineates – the Fair Information Practices – have been written into law in almost every industrialized nation. They are the baseline best practices for anyone who gathers personal information – including governments and corporations. The practices require transparent descriptions of the information collected and grant the data subject control over how information is used and shared.¹

The Privacy Act translates the fair information practices into a series of federal agency responsibilities and rights for individual citizens. Specifically, the Act controls when records can be collected and when and how they can be disclosed; allows individuals to access and correct their own records; and requires agencies to notify people about these systems and keep secure, accurate records.

However, even with this strong foundation, significant challenges have arisen in protecting personal privacy in the United States, including the data held by federal agencies. Some of these challenges arise from the age of the Privacy Act. Congress has not kept the Act up to date with existing technologies and new methods of disclosures such as data breach notification. Other challenges come from agency efforts to circumvent the Act through common practices such as boilerplate notices and the widespread use of commercial information. Still others arise from new court decisions that limit the recovery of damages under the Act.

Many of these problems are highlighted by the National Counterterrorism Center's (NCTC) recent decision claiming wide ranging authority to collect and use the personal, non-terrorist, information of innocent Americans for counterterrorism and law enforcement investigations.

This testimony is divided into four parts:

1. Updates to the Privacy Act;
2. Federal data breach notification;
3. Privacy Act remedies and oversight; and

¹ The full description of these principles can be found here: OECD, *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data* (Sept. 23, 1980).

4. Increased use of non-terrorism related information by the National Counterterrorism Center

I will discuss each of these problems in turn and provide recommendations to eliminate or mitigate them.

II. Updates to the Privacy Act

In 2008, this committee held a hearing, *Protecting Personal Information: Is the Federal Government Doing Enough?*, which explored many of the longstanding problems with the Privacy Act. Specifically, the testimony of Ari Schwartz from the Center for Democracy and Technology described several problems with the Privacy Act and privacy protections across federal agencies.² These issues have also been the focus of numerous studies by the US Government Accountability Office (GAO).³ Longstanding issues include:

- the limited definition of “system of records”,
- overuse of the “routine use” exception,
- failure to extend the protections of the Privacy Act to the government’s use of commercial databases,
- shortcomings in agency compliance with the requirements of the E-Government Act of 2002 in regard to promulgating Privacy Impact Assessments, and
- the lack of privacy leadership at the Office of Management and Budget (OMB) and in some agencies.

Each of these problems persists four years later. I expect other members of the distinguished panel to describe them in detail. Rather than duplicate those efforts I will briefly highlight some key areas of focus.

System of records. The Privacy Act regulates “systems of records” and anything that falls outside of that scope is not regulated by the Act.⁴ Unfortunately, this definition is unduly restrictive because it is tied to the process of retrieving information about a specific individual or information tied to that individual. Current technologies allow for a variety of search techniques using a range of criteria that are not tied to an individual. In discussing this problem, the GAO has noted “a data-mining system that performs analysis by looking for patterns in personal

² *Protecting Personal Information: Is the Federal Government Doing Enough?*: Hearing before the S Committee on Homeland Security and Governmental Affairs, 110th Cong. (2008) (Statement of Ari Schwartz, Vice President, Center for Democracy & Technology) available at: <http://www.hsgac.senate.gov/hearings/protecting-personal-information-is-the-federal-government-doing-enough>

³ GAO, *Congress Should Consider Alternatives for Strengthening Protection of Personally Identifiable Information* GAO-08-795T (Washington D.C.: Jun 18, 2008); GAO, *Agencies Should Ensure That Designated Senior Officials Have Oversight of Key Functions*, GAO-08-603, (Washington D.C.: May 30, 2008).

⁴ System of records is defined as “a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual” 5 U.S.C. 552a(a)(5).

information located in other systems of records or that performs subject-based queries across multiple data sources may not constitute a system of records under the act.”⁵

Routine Use. The routine use exception to the Privacy Act’s disclosure provisions allows agencies to disclose information from systems of records without first obtaining consent from the individuals whose privacy is impacted. Although Congress intended this exception to permit records sharing only when “proper and necessary,”⁶ the exception has become a catchall used to justify a wide array of disclosures. Seemingly, agencies are bound only by what they publish in the Federal Register as a routine use. The statutory requirement that disclosures be “compatible with the purpose for which [the information] was collected”⁷ has been largely ignored. Thus, in practice, the routine use exception serves to circumvent the purpose of the Privacy Act by allowing disclosures at an agency’s whim.

Commercial Databases. The Privacy Act does not extend to the federal government’s use of commercial databases, despite the fact that such use has become widespread and prolific.⁸ These databases frequently contain incorrect information and offer few of the protections, such as access, notice, correction and purpose limitations, which are fundamental to the Privacy Act and fair information practices. In spite of these shortcomings, commercial databases are often accessed for a wide variety of purposes by law enforcement and other agencies, including as part of background check investigations.⁹

Privacy Act Notifications. While agencies have made improvements in providing Privacy Impact Assessments (PIA) and System of Record Act Notices (SORN) for their databases, these notifications are frequently hard to find and often consist of boilerplate language which does a poor job of describing the actual uses of the database and how they handle personal information.¹⁰ This information is sometimes scattered across agency websites and is difficult to find and understand.

Agency Leadership on Privacy. Since 2005 when agency privacy officers’ authority was expanded and formalized, agencies have made strides in adding expertise and leadership on privacy.¹¹ However, in too many agencies, the title of Chief Privacy Officer is held by a senior agency level official such as the Chief Information Officer or General Counsel, but the actual

⁵ GAO-08-795T, page 15.

⁶ LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974: SOURCE BOOK ON PRIVACY 967 (Joint Comm. on Gov’t Operations ed., 1976) available at http://www.loc.gov/frd/Military_Law/pdf/LH_privacy_act-1974.pdf.

⁷ 5 U.S.C. § 552(a)(7).

⁸ See for example GAO, *Privacy: Government Use of Data From Information Resellers Could Include Better Protections*, GAO-08-543T (Washington D.C.: March 11, 2008).

⁹ For more please see the ACLU statement on regulation of data aggregators: <http://www.aclu.org/technology-and-liberty/letter-support-s-1490-personal-data-privacy-and-security-act>

¹⁰ United States. White House. Office of Management and Budget. *Fiscal Year 2011 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002*. Washington: GPO, 2012.

¹¹ 42 USC 2000ee-1.

privacy related responsibilities are handled by a much lower ranking official. Similarly, in spite of OMB's wide ranging responsibilities over privacy, the agency maintains no central privacy officer. These deficiencies result in fragmentation of the responsibility for maintaining privacy protections and uneven compliance with privacy related statutes and regulations.¹²

Recommendation: Each of these important and longstanding problems would be addressed in significant part by S.1732, Privacy Act Modernization for the Information Age Act of 2011. The ACLU believes passage of the portions of this legislation addressing these issues would be an important step forward in updating the Act and improving privacy in federal agencies.

III. Federal data breach notification

Breaches of data are an ongoing and serious problem. According to records compiled by Privacy Rights Clearinghouse, since 2008 at least 78 breaches of information held by federal agencies have occurred, compromising at least 77 million records.¹³ However, existing OMB guidance on data breaches at federal agencies is inadequate and leaves too much discretion to individual agencies in determining whether to disclose breaches.

Relying on the Privacy Act as well as federal data privacy laws, the OMB memorandum *Safeguarding Against and Responding to the Breach of Personally Identifiable Information (M-07-16)* directs federal agencies to implement a data breach notification policy by September 22, 2007 and outlines the framework for doing so.¹⁴ The memorandum is split into four parts, each titled "attachment," which cover the treatment of personally identifiable information (PII), security requirements, outside notification in cases of a breach, and consequence of failures in agency compliance. This guidance only applies to federal executive agencies.

There is significant room for improvement in this guidance. On the positive side, it is mandatory for all agencies, requires basic security protections such as encryption, and advocates that agencies adopt privacy best practices such as data minimization and access limitations. It also prescribes a review of existing databases to assure that their contents are still relevant and necessary and requires the elimination of unnecessary uses of social security numbers. These requirements are particularly important for controlling sensitive information and reducing identity theft.

Where major problems arise with the guidance is in its recommendations for when affected individuals should be notified in the event of a data breach. In contrast to many state

¹² GAO, *Privacy: Agencies Should Ensure That Designated Senior Officials Have Oversight of Key Functions*, GAO-08-603 (Washington D.C.: May 2008).

¹³ *Chronology of Data Breaches*, Privacy Rights Clearing House, <http://www.privacyrights.org/data-breach> (unselect BSO, BSF, BSR, EDU and MED, unselect years 2005-2007, then hit "go").

¹⁴ Office of Management and Budget, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007 (M-07-16).

data breach laws which mandate disclosure whenever data is lost, the OMB guidance describes an elaborate risk based trigger where the agency is required to evaluate a series of factors before determining whether to provide notification. In and of itself this type of discretion is very troubling. By their very nature data breaches are embarrassing events for agencies (or any entity) because they often reveal mistakes or poor security practices. Making notice discretionary will give the agency a strong incentive to come down on the side of not providing notice.

The factors and guidance OMB offers agencies in making this determination only exacerbate this problem. For example, part of the background OMB offers to the agency in deciding whether to disclose a breach is:

“**Chilling Effects of Notices.** A number of experts have raised concerns about unnecessary notification and the chilling effect this may have on the public. In addition, agencies should consider the costs to individuals and businesses of responding to notices where the risk of harm may be low. Agencies should exercise care to evaluate the benefit of notifying the public of low impact incidents.¹⁵”

It is hard to see how this guidance comports with the fundamental Privacy Act principle of transparency and accurate description of disclosures of records. In fact, it seems like an active invitation to defer notice.

The key criteria OMB offers for determining whether to provide notice are equally problematic. As an initial matter, OMB frames all breach notification requirements in terms of whether the breach is likely to cause harm and the level of risk associated with that harm. While harm is an important criteria, it ignores the other important role that public breach notification plays, namely as an accountability tool that spurs improved security and privacy controls. Small breaches are often indicative of a larger problem in computer security practices, training or other controls. Allowing agencies to paper over those problems is likely to lead to greater problems down the road.

Further, OMB’s evaluation of what might cause harm is flawed. It encourages agencies to consider factors like:

the effect of a breach of confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.¹⁶

¹⁵ *Id* at 12-13.

¹⁶ *Id* at 15.

These decisions are best made by the individual affected, not the agency. In reality, it is impossible to see how the agency could foresee secondary uses of data. Sometimes even data that most people view as benign, such as name and address, can be very sensitive if associated with a survivor of sexual assault or stalking who has worked very hard to conceal it.

The guidance also authorizes the agency to consider whether the risk can be mitigated by the agency. Naturally the agency should take all mitigation steps but that effort should be completely separate from a decision about whether to notify victims of a breach. Again, all of this guidance is completely contrary to the fundamental purpose of the Privacy Act: to empower citizens with knowledge about and control over how the government handles their personal information.

Recommendation: OMB should change its data breach guidance to severely limit the discretion of federal agencies to avoid providing notice to affected parties in the case of a breach. Notice should be triggered whenever personally identifiable data is released in a readable form (not protected by encryption or other security measures).

IV. Privacy Act Remedies and Oversight

Since 2008, there have been two significant developments which have served to further erode transparency and accountability under the Privacy Act – the recent Supreme Court case *FAA v. Cooper* and the failure by the President and Congress to fill the Privacy and Civil Liberties Oversight Board (PCLOB).

A. *FAA v. Cooper*

In *FAA v. Cooper*, the Supreme Court held that the victims of Privacy Act violations cannot recover damages for mental or emotional distress, no matter how severe, unless they suffer financial harm as a result of the violation.¹⁷ In *Cooper*, the plaintiff's HIV status was shared by the Social Security Administration with the Federal Aviation Administration (FAA) and Department of Transportation.

In *Cooper*, despite the fact that the agencies violated the Privacy Act, it was unclear whether the plaintiff could recover the damages authorized by 5 U.S.C. 552(a)(g)(4)(A). This section provides that any agency who willfully fails to comply with the Privacy Act is liable for "actual damages sustained by the individual as a result of the... failure, but in no case shall a person entitled to recovery receive less than the sum of \$1,000." At issue was the definition of "actual damages." In previous decisions, circuits had split over whether "actual damages" meant "general damages," which allow recovery for emotional harm, or "special damages," which required pecuniary harms.¹⁸ This definition was important because the plaintiff did not allege an

¹⁷ *F.A.A. v. Cooper*, 132 S. Ct. 1441 (2012).

¹⁸ See *Fitzpatrick v. IRS*, 665 F.2d 327, 329-31 (11th Cir.1982) (holding that "actual damages" are limited to proven pecuniary losses); *Johnson v. IRS*, 700 F.2d971, 972 (5th Cir. 1983) (holding that "actual damages" may be

economic loss as a result of the Privacy Act violation. He only claimed to have suffered “humiliation, embarrassment, mental anguish, fear of social ostracism and other severe emotional distress.”¹⁹ The Court concluded that Congress intended through use of the term “actual damages” to mean special damages and limited the availability of recovery under the Privacy Act to those suffering from economic harm. The plaintiff was denied damages for his emotional harm.

This decision has a negative impact on the general privacy protections provided by the Act, as well as on an individual’s ability to recover for harms. The Privacy Act was created in order to provide “a series of basic safeguards... to help remedy the misuse of personal information by the Federal Government and reassert the fundamental rights of personal privacy of all Americans.”²⁰ Congress viewed the civil damages remedy as key to enforcing the Act and as commentators have noted the deterrent effect presented by the threat of litigation is a significant one.²¹ By foreclosing relief for these types of harms, the court weakens protections for precisely the type of harmful disclosure of embarrassing or detrimental information, such as HIV status, that should be a core focus of the Act.

The decision also strips from victims of real harms the ability to recover their damages. The court’s holding is clear. No matter how much emotional pain, humiliation or real mental distress a victim endures, if it is not a pecuniary harm, recovery is barred. In practice the result of this interpretation is that release of much of the information covered by the Privacy Act will fall outside the statutory remedy. For example, recently it was alleged that the 2010 campaign of Washington, D.C. Mayor Vincent Gray improperly used lists of residents of public housing as part of its get out the vote efforts.²² These lists would be covered by the Privacy Act and contain names, addresses and phone numbers including cell phones. If public housing residents were harmed by this disclosure, for example by receiving harassing phone calls, under *Cooper* they would have no remedy absent a showing of financial harm.

Recommendation: The language of the Privacy Act should be modified in 5 U.S.C. 552a(g)(4)(A) to make clear that actual damages extend beyond pecuniary harms and include mental and emotional distress.

B. Privacy and Civil Liberties Oversight Board

established by evidence of either financial or non-financial injuries); *Hudson v. Reno*, 130 F.3d 1193, 1206-07 (6th Cir. 1997) (holding that “actual damages” can be established only by evidence pecuniary losses).

¹⁹ *Cooper* at 1447.

²⁰ *House Comm. on Gov’t Operations and Senate Comm. on Gov’t Operations*, 94th Cong., 2d Sess., Legislative History of the Privacy Act of 1974 -- S. 3418 (Pub. L. No. 93-579) Source Book on Privacy, 304 (1976) available at http://www.ioc.gov/rr/frd/Military_Law/pdf/LH_privacy_act-1974.pdf.

²¹ Frederick Z. Lodge, *Damages Under the Privacy Act of 1974: Compensation and Deterrence*, 52 *Fordham L. Rev.* 611, 622 (1984).

²² Nikita Stewart and Mike DeBonis, *Mayor Gray’s 2010 campaign had database of public-housing residents*, *Washington Post*, July 22, 2012.

At the recommendation of the 9/11 Commission, in 2004, Congress created the Privacy and Civil Liberties Oversight Board (PCLOB) and later reconstituted it as an independent body in 2007.²³ The PCLOB is tasked with overseeing “the information sharing practices of the departments, agencies, and elements of the executive branch relating to efforts to protect the Nation from terrorism to determine whether they appropriately protect privacy and civil liberties”.²⁴ As such, it has significant oversight authority regarding the type of collection and sharing of personal information regulated by the Privacy Act and could serve as an important check on abuses of the Act.

Unfortunately, President Bush refused to nominate one of the candidates put forth by leaders in Congress who traditionally select the commissioners from the opposite party from the president. In retaliation, the Senate refused to confirm any of Bush’s GOP nominees. Because the terms of the original board members expired in January 2008, the revised board was never brought into existence during President Bush’s term.²⁵

Compliance has been no better under President Obama. Despite letters from lawmakers and advocacy groups, he failed to nominate a full slate of candidates for the Board for almost three years. It wasn’t until December 2011 that nominations were sent to the Senate for its consideration.²⁶ Candidates for the PCLOB have been awaiting action by the full Senate since May.

Given that the board has never existed in its current form it is hard to concretely evaluate the impact it would have on Privacy Act enforcement, however it was a key recommendation of the 9/11 Commission. As the former Chairman Tom Kean and Vice Chairman Lee Hamilton testified before this committee:

If we were issuing grades, the implementation of this recommendation would receive a failing mark. We urge the Administration and Congress to address this failure in a speedy fashion. An array of security-related policies and programs present significant privacy and liberty concerns. A robust and visible Board can help reassure Americans that these programs are designed and executed with the preservation of our core values in mind.

²³ U.S. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington: GPO, 2004), p. 395. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-408 (2004); Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, Title VIII, § 801 (2007).

²⁴ The 9/11 Commission Act of 2007 §801 (d)(2)(B).

²⁵ Michael Isikoff and Mark Hosenball, “Who’s Watching the Spies?” *Newsweek*, July 9, 2008; online at <http://www.newsweek.com/id/145140>.

²⁶ The White House, Office of the Press Secretary, *President Obama Announces More Key Administration Posts*, December 15, 2011.

Board review can also give national security officials an extra degree of assurance that their efforts will not be perceived later as violating civil liberties.²⁷

While it is unknown how much oversight the PCLOB will eventually exert, it is incontrovertible that it will be impossible for the Board to provide any oversight until members are nominated and confirmed.

Recommendation: Nominate and confirm a full slate of board members for the PCLOB and fully staff this vital independent board.

V. Increased use of non-terrorism related information by the National Counterterrorism Center

The steady erosion of privacy protections for personal information held by the federal government has led to an environment where information on Americans can be shared widely for a host of purposes unrelated to the original reason it was collected. Perhaps the most troubling recent example of this trend is the sweeping changes the National Counterterrorism Center (NCTC) made to its guidelines governing how it collects and uses information about US persons not suspected of wrongdoing for intelligence analysis.²⁸ The new rules effectively remove traditional protections for US person information and allow the vast power of the US Intelligence Community to be turned on innocent Americans. They clearly demonstrate the need to update the Privacy Act and ensure that Americans have real protections for how the information collected by an array of federal government agencies is shared and used.

A. Changes to the NCTC Guidelines

Under the new guidelines approved by the Attorney General, NCTC may engage in a variety of troubling new practices including collecting entire databases from federal agencies which mainly consist of information about Americans with no connection to terrorism, and analyzing those databases and disseminating the results for reasons which are also unconnected to terrorism.

The new guidelines accomplish this in a variety of ways. In what is perhaps the most significant change, the Obama administration has extended the authority of the NCTC to intentionally collect, retain and assess data on U.S. citizens and residents, even where those people have no suspected ties to terrorism. Previously, the intelligence community was barred from collecting information about ordinary Americans unless the person was a terror suspect or related to an actual investigation. Therefore, when NCTC collected information from federal

²⁷ *Ten Years After 9/11: A Report From the 9/11 Commission Chairmen, before the Senate Committee on Homeland Security and Governmental Affairs*, 112th Congress, (2011) (Testimony Governor Tom Kean and Congressman Lee Hamilton).

²⁸ National Counterterrorism Center, GUIDELINES FOR ACCESS, RETENTION, USE, AND DISSEMINATION BY THE NATIONAL COUNTERTERRORISM CENTER AND OTHER AGENCIES OF INFORMATION IN DATASETS CONTAINING NON-TERRORISM INFORMATION, Released March 22, 2012.

government databases, it had to search for and identify any innocent US person information inadvertently collected, and discard it within 180 days. This crucial purpose limitation meant that NCTC was dissuaded from collecting or maintaining information on innocent Americans in its large databases, and prohibited from using or disseminating it. The 2012 guidelines eliminate this check, allowing NCTC to collect and “continually assess” information on innocent Americans for up to five years.²⁹

The new guidelines also effectively broaden an authority previously claimed by NCTC, namely the ability to ingest entire databases maintained by other government agencies. According to the new guidelines, as long as the Director of the NCTC determines that a dataset contains “significant terrorism information,” which is not defined, the NCTC may “acquire and replicate portions or the entirety of a dataset”. While NCTC previously claimed such authority, the retention limits on collection for US persons meant that only datasets consisting almost entirely of terrorism information and/or non-US person information could reasonably be collected using this methodology. The NCTC was dissuaded from swallowing up entire databases consisting of large amounts of innocent US person information by the resource burden of locating and purging it within 180 days. By allowing collection and retention of non-terrorism related US person information for 5 years, the NCTC Guidelines have authorized the NCTC to ingest many new federal databases that consist primarily of non-terrorism related US person information.³⁰

Once NCTC acquires this information, the new guidelines give it broad new powers to search through it. As long as queries are designed to solely identify information that is reasonably believed to constitute terrorism information, it may conduct queries that involve non-terrorism data points and pattern based searches and analysis (data mining).³¹ It is particularly noteworthy that NCTC relies on a technique, data mining, which has been thoroughly discredited as a useful tool for identifying terrorists. Data mining searches are notoriously inaccurate and prone to false positives, and it is therefore very likely that individuals with no connection to terrorism will be caught up in terrorism investigations if this technique is utilized. As far back as 2008 the National Academy of Sciences found that data mining for terrorism was scientifically “not feasible” as a methodology, and likely to have significant negative impacts on privacy and civil liberties.³²

Equally disturbing is that once information is gathered and assessed with these tools it can be shared very broadly, in some cases with literally anyone. Such sharing does not have to

²⁹ 2012 Guidelines at 9.

³⁰ *Id.*

³¹ *Id.* at 10.

³² See National Academy of Sciences report, “Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment” http://books.nap.edu/catalog.php?record_id=12452#toc

be connected to a terrorism investigation. This chart lists some of the types of information NCTC may share, as well as all the entities that can receive this information:³³

Types of information that can be shared	Individuals and groups that can receive information
Foreign aspects of international narcotics activities	Federal, state, local, tribal, or foreign or international agency that is reasonably believed to need such information
Reasonably appears to be evidence of a crime	Federal, state, local, tribal, or foreign agency which has jurisdiction and that is reasonably believed to need such information
Reasonably believed to be necessary to: (i) protect the safety or security of persons, property, or organizations or (ii) protect against or prevent a crime or a threat to the national security	Federal, state, local, tribal, or foreign entity, or to an individual or entity not part of a government
For the purpose of determining the suitability or credibility of persons who are reasonably believed to be potential sources or contacts	Federal, state, local, tribal, or foreign or international entity
For the purpose of protecting foreign intelligence or counterintelligence sources and methods from unauthorized disclosure	Federal, state, local, tribal, or foreign or international entity
Otherwise required by statutes; treaties; executive orders; Presidential directives; National Security Council directives; Homeland Security Council directives; or Attorney General-approved policies, memoranda of understanding, or agreements	2012 Guidelines are silent on who the sharing would be to, but presumably that would be covered by the statutes, treaties, orders, directives, policies, MOUs or agreements
For the purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it	Appropriate elements of the Intelligence Community
Bulk dissemination in support of a legally authorized counterterrorism mission	Other elements of the Intelligence Community

In short, information can be shared for an almost unlimited number of purposes and to a completely unlimited number of individuals. Particularly striking is the authority to share information with anyone (“federal, state, local, tribal, or foreign entity, or to an individual or

³³ *Id* at 13-14.

entity not part of a government”) in order to protect the safety or security of person, property or organizations; or protect against or prevent a crime or a threat to the national security. Such authority seems to provide few limits and almost no guidance to NCTC and other intelligence agencies.

All of this is happening with very little oversight. Controls over the NCTC are mostly internal to the DNI’s office and important oversight bodies such as Congress and the President’s Intelligence Oversight Board aren’t notified of even “significant” failures to comply with the Guidelines.³⁴ One entity might be able to perform some useful oversight because it does have fairly straightforward authority to “access all relevant NCTC records, reports, audits, reviews, documents, papers, recommendations, and other materials that it deems relevant to its oversight of NCTC activities.” Unfortunately that entity is the PCLOB, which, as described above, has not been seated.

B. Privacy Act Impact

When these practices are viewed through the lens of the supposed protections of the Privacy Act, it is clear how badly the Act is in need of an update. One of the major protections of the Privacy Act is that it bars the sharing of records between agencies except pursuant to specifically delineated exceptions described in subsection (b). None of these exceptions are broad enough to cover this type of wholesale disclosure to the NCTC, nor is there a general national security exception to the Privacy Act. Presumably then, entire databases are being disclosed pursuant to the long abused “routine use” exception described in section II. However, it is difficult to imagine that any American believes that any transaction with the federal government can open them up for screening as a terrorist as long as an agency declares use of that information for that purpose to be “routine”.

Courts have also held that agencies shouldn’t share information with other agencies unless it has compatibility with the purpose for which the information was collected. The modern definition of “compatibility” was established in *Britt v. Naval Investigative Services*, in which the 3rd Circuit held there must be “some meaningful degree of convergence between the agencies’ purpose in collecting the information and its disclosure.”³⁵ The court also noted that the purpose for collection and disclosure should be determined on a case-specific basis. Similarly, in *Swenson v. U.S. Postal Service*, the 9th Circuit echoed *Britt’s* holding, and found that there must be a “meaningful degree of convergence” between the purpose for which the information was collected and the reason it was disseminated.³⁶

³⁴ *Id* at 17.

³⁵ 886 F.2d 544 (3rd Cir. 1989)

³⁶ 890 F.2d 1075 (1989)

The NCTC also asserts a series of other exceptions to the Privacy Act. These types of exemptions are authorized under subparts (j) and (k) of the Act and have become commonplace. But a quick review of the exemptions NCTC asserts demonstrates how much control they take away from the subject of the information. NCTC exempts itself from the following requirements for all its databases:

- Subsection (c)(3) (accounting for disclosures),
- Subsections (d)(1)-(4) (record subject's right to access and amend records),
- Subsection (e)(1) (maintain only relevant and necessary records),
- Subsection (e)(4)(G) and (H) (publication of procedures for notifying subjects of the existence of records about them and how they may access records and contest contents),
- Subsection (e)(4)(I) (identifying sources of records in the system of records), and
- subsection (f) (agency rules for notifying subjects to the existence of records about them, for accessing and amending records, and for assessing fees).³⁷

In short, NCTC will not guarantee it is using accurate information, account for how it discloses that information, assure that it is relevant or ever let individuals know they have been the subject of an investigation. For obvious reasons the accuracy of the information is of particular concern. Evidence from other database where the collecting agency does not attest to the accuracy of the information indicates that this tends to result in substantial errors.³⁸

The federal government collects an enormous amount of personal information. It is necessary in order for citizens to receive benefits and services, to exercise fundamental rights like voting or petitioning the government, for licensing everything from guns to businesses, for employment, education and for many types of health care. In short this information collection is nearly ubiquitous to American life. However under the new NCTC guidelines and the outdated protections of the Privacy Act, providing this information to any federal agency is akin to entering a lineup as a potential terrorist. Nor does the government's sharing this information have to be connected to terrorism at all. Information can be used for national security and safety, drug investigations, if it is evidence of a crime, or simply to evaluate sources or contacts. This boundless sharing is broad enough to encompass disclosures to an employer or landlord about someone who NCTC may think is potentially a criminal, or at the request of local law enforcement for vetting you as a potential informant.

Ultimately, this boundless disclosure, limitless sharing and expansive exemptions seem to create a system of records that is outside the Privacy Act. The only protection offered by the Privacy Act in regard to NCTC is strictly bureaucratic – the agency must declare that a system of records exists and, either explicitly state that many of the provisions of the Privacy Act do not

³⁷ 32 CFR 1701.21

³⁸ See for example errors in the National Crime Information Center (NCIC) which is collected by the FBI: <http://bjs.ojp.usdoj.gov/content/pub/pdf/umchri01.pdf> and http://epic.org/privacy/hiiibel/epic_amicus.pdf

apply or implicitly exploit loopholes to avoid its requirements. Contrast this with the Congressional finding in support of the Privacy Act:

The increasing use of computers and sophisticated information technology, while essential to the efficient operations of the government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information; ... In order to protect the privacy of individuals identified in information system maintained by federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

It is difficult to see how the NCTC's guidelines for handling Americans' personal information meet any of these goals. Unfortunately, this type of broad information sharing is not an isolated occurrence. Instead, broadening definitions of routine use, constant employment of exemptions, use of commercial databases and boilerplate notifications result in a systematic weakening of the Privacy Act and widespread harm to Americans' privacy.

Recommendation: Congress should prohibit the intelligence community's intentional collection of non-terrorism related US person information. If such information is inadvertently collected it should be immediately identified and removed.

VI. Conclusion

The Privacy Act and other associated federal data use practices require an overhaul. Their outdated protections are widely circumvented by agencies and the result is the creation of new databases, such as those compiled by the NCTC that violate the spirit of the Privacy Act and harm Americans' privacy.

STATEMENT

of

Paul Rosenzweig
Red Branch Consulting, PLLC
Professorial Lecturer in Law, George Washington University
Visiting Fellow, The Heritage Foundation
Washington, D.C.

before the

Subcommittee on Oversight of Government Management, the Federal Workforce and the District of
Columbia
Committee on Homeland Security and Governmental Affairs
United States Senate

July 31, 2012

The State of Privacy and Security – Our Antique Privacy Rules

Introduction

Chairman Akaka, Ranking Member Johnson, and Members of the Committee, I thank you for your invitation to appear today and present testimony on the question of data privacy and security under the Privacy Act. My name is Paul Rosenzweig and I am the Principal and founder of a small consulting company, Red Branch Consulting, PLLC, which specializes in, among other things, cybersecurity policy and legal advice. I am also a Senior Advisor to The Chertoff Group and a Professorial Lecturer in Law at George Washington University where I teach a course on Cybersecurity Law and Policy. In addition, I serve as a Visiting Fellow with a joint appointment in the Center for Legal & Judicial Studies and the Douglas and Sarah Allison Center for Foreign Policy Studies at The Heritage Foundation.¹ From 2005 to 2009 I served as the Deputy Assistant Secretary for Policy in the Department of Homeland Security.

¹ The Heritage Foundation is a public policy, research, and educational organization recognized as exempt under section 501(c)(3) of the Internal Revenue Code. It is privately supported and receives no funds from any government at any level, nor does it perform any government or other contract work.

The Heritage Foundation is the most broadly supported think tank in the United States. During 2011, it had nearly 700,000 individual, foundation, and corporate supporters representing every state in the U.S. Its 2011 income came from the following sources:

Individuals	78%
Foundations	17%

Needless to say, my testimony today is in my individual capacity and does not reflect the views of any institution with which I am affiliated or any of my various clients. Much of my testimony today is derived from prior academic work I have done in this field, most notably two research papers I published, one entitled "Privacy and Counter-Terrorism: The Pervasiveness of Data,"² and an older work entitled "Privacy and Consequences: Legal and Policy Structures for Implementing New Counter-Terrorism Technologies and Protecting Civil Liberty."³ I used much of that research and additional work to create a Web-based project entitled "The Data Minefield"⁴ while I was the Carnegie Visiting Fellow at the Medill School of Journalism, Northwestern University in 2011. All of that work, in turn, has been modified and will appear as part of several chapters in my forthcoming book, *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World* (Praeger Press 2012).

In my testimony today I want to make four basic points:

- The extent to which personal information is available due to society's increasing use and reliance on technology is growing every day. While one may view this as a good thing or a bad thing, it is, I submit, an inevitable thing. Wishing that it were not so is like King Canute commanding the tide not to come in. In the long run we do a disservice to our citizens if we do not recognize this reality.
- Thus, my second point is that it is, in my judgment, a mistake to speak of balancing privacy and information sharing in today's post-9/11 technological world. Rather, our objective should be to maximize both values. But this requires us to recognize that there is more than one way to protect privacy and that our current model of privacy is outdated and antiquated. Thus, while I am sure that all on this panel will agree that the Privacy Act needs to be updated, I suspect that my own views on how to do so are far more radical and transformative than those of my colleagues.
- In my view, the government can best ensure the privacy of the citizens by abandoning concepts like the Fair Information Practices that are tied to older technological conceptions. Instead of focusing on use and purpose limitations that are inconsistent with current capabilities and the threat environment (which requires the use of advanced data analytics) we would be better to focus privacy rules on the (admittedly more difficult) question of defining when it is and is not

Corporations 5%

The top five corporate givers provided The Heritage Foundation with 2% of its 2011 income. The Heritage Foundation's books are audited annually by the national accounting firm of McGladrey & Pullen. A list of major donors is available from The Heritage Foundation upon request.

Members of The Heritage Foundation staff testify as individuals discussing their own independent research. The views expressed are their own and do not reflect an institutional position for The Heritage Foundation or its board of trustees.

² 42 Case W. Res. J. Int'l L. 625 (2010).

³ Robert Popp & John Yen, eds., *Emergent Information Technologies and Enabling Policies for Counter-Terrorism* (Wiley-IEEE 2006).

⁴ <http://nationalsecurityzone.org/datamining/>.

appropriate to impose adverse consequences on citizens, combined with the equally essential (and also difficult) task of building a comprehensive oversight and audit system that constrains government activity effectively.

- It follows from what I've said already that I would not advise the Congress to undertake the task of updating the Privacy Act. Since I think that its entire structure is mismatched to technological reality, I would advocate a more extended consideration that leads to a complete rewrite of the statute along the lines I outline below.

Dataveillance and Cyber Conflict

Cyberspace is the natural battleground for enhanced analytical tools that are enabled by the technology of data collection. If our goal is to combat terrorists or insurgents (or even other nations) then the cyber domain offers us the capacity not just to steal secret information through espionage, but to take observable public behavior and information and use cyber tools to develop a more nuanced and robust understanding of their tactics and intentions. Likewise, it can be used by our opponents to uncover our own secrets.

Traditionally, the concept of "surveillance" has been taken to mean an act of physical surveillance—e.g., following someone around or planting a secret camera in an apartment. As technology improved, our spy agencies and law enforcement institutions increasingly came to rely on even more sophisticated technical means of surveillance,⁵ and so we came to develop the capacity to electronically intercept telecommunications and examine email while in transit.⁶

To these more "traditional" forms of surveillance we must now add another: the collection and analysis of personal data and information about an individual or organization. Call the phenomenon "dataveillance" if you wish, but it is an inevitable product of our increasing reliance on the Internet and global communications systems. One leaves an electronic trail almost everywhere you go. Increasingly, in a networked world technological changes have made personal information pervasively available. As the available storehouse of data has grown, so have governmental and commercial efforts to use this personal data for their own purposes. Commercial enterprises target ads and solicit new customers. Governments use the data to, for example, identify and target previously unknown terror suspects—to find so-called clean skins who are not in any intelligence database. This capability for enhanced data analysis has already proven its utility and holds great promise for the future of commercial activity and counter-terrorism efforts.

⁵ For an overarching history of the transition from human intelligence to U-2 spy planes and, eventually, to satellites, see generally Tim Weiner, *Legacy of Ashes: The History of the CIA* (2007).

⁶ Law enforcement electronic interceptions are generally governed by Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified in scattered sections of 5, 18, and 42 U.S.C.), and intelligence interceptions are governed by the Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C.).

Yet this analytical capacity also comes at a price—the peril of creating an ineradicable trove of information about innocent individuals. That peril is typically supposed to stem from problems of misuse; in the government sphere one imagines data mining to identify political opponents, and in the private sector we fear targeted spam. To be sure, that is a danger to be guarded against.

But the dangers of pervasively available data also arise from other factors. Often, for example, there is an absence of context to the data that permits or requires inaccurate inferences. Knowing that an individual has a criminal conviction is a bare data point; knowing what the conviction was for and in what context allows for a more granular and refined judgment.

The challenges arising from these new forms of analysis have already become the subject of significant political debate. One need but think of the controversy surrounding the most ambitious of these—the Total Information Awareness (TIA) program. TIA was a research program initiated by the Defense Advanced Research Projects Agency (DARPA) in the immediate aftermath of September 11. Its conception was to use advanced data analysis techniques to search the information space of commercial and public sector data looking for threat signatures that were indicative of a terrorist threat. Because it would have given the government access to vast quantities of data about individuals, it was condemned as a return of “Big Brother.”⁷

Compare that condemnation with the universal criticism of the government for its failure to “connect the dots” during the Christmas 2009 bomb plot attempted by Umar Farouk Abdulmutallab.⁸ This gives you some idea of the crosscurrents at play. The conundrum arises because the analytical techniques are fundamentally similar to those used by traditional law enforcement agencies, but they operate on so much vaster a set of data, and that data is so much more readily capable of analysis and manipulation, that the differences in degree tend to become differences in kind. To put the issue in perspective, just consider a partial listing of relevant databases that might be targeted: credit card, telephone calls, criminal records, real estate purchases, travel itineraries, and so on.

One thing is certain—these analytical tools are of such great utility that governments will expand their use, as will the private sector. Old rules about collection and use limitations are no longer technologically relevant. If we value privacy at all, these ineffective protections must be replaced with new constructs. The goal then is the identification of a suitable legal and policy regime to regulate and manage the use of mass quantities of personal data.

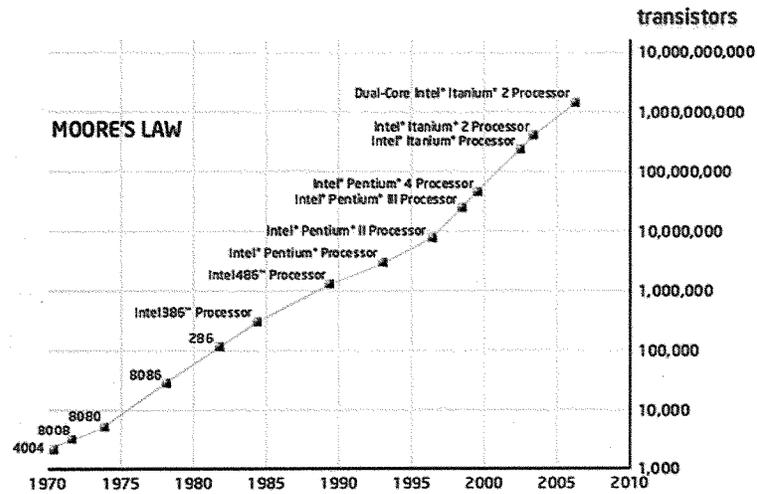
⁷ An article by William Safire instigated a significant political controversy. See William Safire, “You Are a Suspect,” *The New York Times*, Nov. 14, 2002, at A35. It led directly to the creation of a blue-ribbon panel, the Technology and Privacy Advisory Committee, and, eventually, to the cancellation of the Total Information Awareness program. The final report of the Technology and Privacy Advisory Committee is available at <http://www.defense.gov/news/Jan2006/d20060208tapac.pdf> (last visited Feb. 23, 2010).

⁸ See, e.g., Scott Shane & Eric Lipton, “Passengers’ Actions Thwart a Plan to Down a Jet,” *The New York Times*, Dec. 27, 2009, at A1.

The Computing and Storage Revolution

The growth of dataveillance is inevitable. It reflects a fundamental change caused by technological advances that, like King Canute's fabled tide, cannot be stopped or slowed. Increasingly, the cyber conflict will be fought, and won, by those who use data to their best advantage. The opportunity—or problem, depending on one's perspective—derives from two related, yet distinct trends: increases in computing power and decreases in data storage costs.

Many are familiar with the long-term increase in the power of computers. It is most familiarly characterized as Moore's Law—named after Intel computer scientist Gordon Moore, who first posited the law in 1965. Moore's Law predicts that computer chip capacities will double every eighteen to twenty-four months.⁹ Moore's law has been remarkably constant for nearly thirty years, as the graph below demonstrates.¹⁰



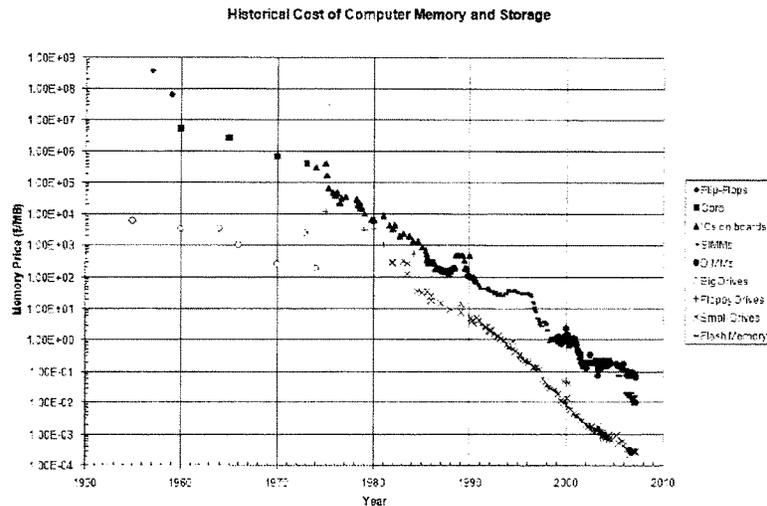
The scale makes clear that the effect of routine doubling is logarithmic. Processor capacity today is roughly more than one million times faster than processor speed in 1970.

⁹ See Linda Null & Julia Lobur, *The Essentials of Computer Organization and Architecture* 27 (2d ed. 2006).

¹⁰ Charts of Moore's law are widely available. This one is from <http://www.deepspare.com/images/MooresLaw.jpg> (last visited Feb. 23, 2010).

The power of this processing capacity—which translates almost directly into processing speed—is immense. And though no one predicts that processing speed will double indefinitely—surely a physical impossibility—there is no current expectation that the limits of chip capacity have been reached.

To this trend one must also add the remarkable reduction in the costs of data storage. As the following chart demonstrates,¹¹ data storage costs have also been decreasing at a logarithmic rate, almost identical to the increases we have experienced in chip capacity, but with an inverse slope.



What this means in practical terms is that in 1984—less than thirty years ago—it cost roughly two hundred dollars to store a megabyte of data. By 1999 that cost had sunk to seventy-five cents. Today you can buy one hundred megabytes of data storage capacity for a penny. On eBay you can frequently purchase a terabyte storage device for your desktop for under one hundred dollars. A terabyte is roughly 1 trillion bytes of data—a huge volume for storing simple alphanumeric information. Here, too, the prospects are for ever-cheaper data storage. One can readily imagine peta-, exa-, or even yottabyte sized personal storage devices.¹² If that is for the individual, imagine what a large corporation or a government can purchase and maintain.

¹¹ Lev Lafayette, "Definition, History, Usage and Future of Computer Data Storage," *Organdi*, http://organdi.net/article.php3?id_article=82 (the graph is directly available at http://organdi.net/IMG/gif/historical_cost_graph5.gif).

¹² A petabyte is 1000^5 bytes, an exabyte is 1000^6 bytes, and a yottabyte is 1000^8 bytes.

Therefore, the story of technology today requires us to answer the question: “What happens when ever-quicker processing power meets ever-cheaper storage capacity?” Anyone who uses Gmail knows the answer to that question. No longer do you have to laboriously label, file, and tag your email. One may now simply store all the email he or she wants to retain and use a simple natural language search algorithm to pull up relevant emails from storage when needed. The storage cost of Gmail to the user is zero—Google offers it for free—and the processing time for any search request for the average individual is measured in, at most, seconds, not minutes.

Here is how IBM Chairman Samuel J. Palmisano put it in a speech he gave in September 2011:

We’re all aware of the approximately two billion people now on the Internet—in every part of the planet, thanks to the explosion of mobile technology.

But there are also upwards of a trillion interconnected and intelligent objects and organisms—what some call the Internet of Things.

All of this is generating vast stores of information. It is estimated that there will be 44 times as much data and content coming over the next decade...reaching 35 zettabytes in 2020. A zettabyte is a 1 followed by 21 zeros. And thanks to advanced computation and analytics, we can now make sense of that data in something like real time. This enables very different kinds of insight, foresight and decision-making.¹³

In other words, we live in the world of “Big Data.” Data is now pervasively available and pervasively searchable. For large-scale databases of the size maintained by governments or companies, the practical limitations lie in the actual search algorithms used and how they are designed to process the data, not in the chips or the storage units. The changes that will come from this new cyber reality are profound.

The Power of Data Analytics

Ten years ago, surveying the technology of the time—which, by and large, was one hundred times *less* powerful than today’s data processing capacity—Scott McNealy, then-CEO of Sun Microsystems, said, “Privacy is dead. Get over it.”¹⁴ He was, it seems, slightly wrong. Pure privacy—that is, the privacy of activities in your own home—remains reasonably well-protected.¹⁵ What has been lost, and will become even more so increasingly, is the anonymity of being able to act in public (whether physically or in cyberspace) without anyone having the technological capacity to permanently record and retain data

¹³ Samuel J. Palmisano, “Thoughts on the Future of Leadership,” September 20, 2011, https://www.ibm.com/smarterplanet/us/en/leadership/stories/pdf/prepared_remarks.pdf.

¹⁴ Though the original statement may be apocryphal, many have quoted it since, including McNealy himself. See, e.g., Matt Hambien, “McNealy Calls for Smart Cards,” *Computer World*, Oct 12, 2001, http://www.computerworld.com/s/article/64729/McNealy_calls_for_smart_cards_to_help_security.

¹⁵ See, e.g., *Kyllo v. United States*, 533 U.S. 27 (2001) (the use of thermal imaging outside the home without a warrant is an illegal search when it is used, even indirectly, to reveal activity taking place within the home).

about your activity for later analysis. Today, large data collection and aggregation companies, such as Experian and Axicom, may hire retirees to harvest, by hand, public records from government databases.¹⁶ Paper records are digitized and electronic records are downloaded. These data aggregation companies typically hold birth records, credit and conviction records, real estate transactions and liens, bridal registries, and even kennel club records. One company, Acxiom, estimates that it holds on average approximately 1,500 pieces of data on each adult American.¹⁷

Since most, though not all, of these records are governmental in origin, the government has equivalent access to the data, and what they cannot create themselves they can likely buy or demand from the private sector. The day is now here when anyone with enough data and sufficient computing power can develop a detailed picture of any identifiable individual. That picture might tell your food preferences or your underwear size. It might tell something about your terrorist activity. Or your politics.

This analytical capacity can have a powerful influence in law and policy—and in particular in revealing links between the cyber personas and the real world activities of individuals. When we speak of the new form of “dataveillance,” we are not speaking of the comparatively simple matching algorithms that cross check when a person’s name is submitted for review—when, for example, they apply for a job. Even that exercise is a challenge for any government, as the failure to list Abdulmutallab in advance of the 2009 Christmas bombing attempt demonstrates.¹⁸ The process contains uncertainties of data accuracy and fidelity, analysis and registration, transmission and propagation, and review, correction, and revision. Yet, even with those complexities, the process uses relatively simple technology—the implementation is what poses a challenge.

By contrast, other systems of data analysis are far more technologically sophisticated. They are, in the end, an attempt to sift through large quantities of personal information to identify subjects when their identities are not already known. In the commercial context, these individuals are called “potential customers.” In the cyber conflict context, they might be called “Anonymous” or “Russian patriotic hackers.” In the terrorism context, they are often called “clean skins” because there is no known derogatory information connected to their names or identities. In this latter context, the individuals are dangerous because nothing is known of their predilections. For precisely this reason, this form of data analysis is sometimes called “knowledge discovery,” as the intention is to discover something previously unknown about an individual. There can be little doubt that data analysis of this sort can prove to be of great value. A few examples will illustrate the point.

¹⁶ I learned this from discussions with ChoicePoint’s CEO Derek Smith and other industry practitioners. See also Ralph M. Stair & George W. Reynolds, *Fundamentals of Information Systems* 362 (2003) (discussing Experian’s collection of public records from government databases).

¹⁷ Stephanie Clifford, “Online Ads Follow Web Users, and Get Much More Personal,” *The New York Times*, July 30, 2009, at A1.

¹⁸ Peter Baker & Carl Hulse, “Obama Hears of Signs That Should Have Grounded Plot,” *The New York Times*, Dec. 30, 2009, at A1.

The story of Ra'ed al-Banna, a Jordanian who attempted to enter the U.S. at O'Hare Airport on June 14, 2003, illustrates the value of computer dataveillance.¹⁹ al-Banna was carrying a valid business visa in his Jordanian passport and, on the surface, appeared to be an unremarkable business traveler from the Middle East.

The Department of Homeland Security operates a sophisticated data analysis program called the Automated Targeting System (ATS) to assess the comparative risks of arriving passengers. Based on those assessments, the inspection resources of Customs and Border Protection (CBP) are allocated.²⁰ The system is essential given the sheer volume of travelers to America. In a typical year approximately three hundred and fifty million people sought entry across our borders, and more than eighty-five million of those arrived by air.²¹ Since over three hundred and fifty million individuals cannot, obviously, be subject to intense scrutiny, some form of assessment and analysis must be used to make choices about how and when to conduct inspections. ATS is that system.

ATS flagged al-Banna for heightened scrutiny.²² His pattern of travel and his prior record of entry to the U.S. combined to suggest that he should be subjected to secondary screening—a form of enhanced, individualized review where a passenger is pulled from the main line of entrants and individually questioned. During the secondary interview, al-Banna's answers were inconsistent and evasive—so much so that the CBP officer who conducted the interview decided to deny his application for entry and ordered him returned to his point of origin.²³ As a matter of routine, al-Banna's photograph and fingerprints were collected before he was sent on his way.

There the story might have ended, since CBP officers reject entry applications daily for a host of reasons, but al-Banna proved an unusual case. More than a year later, in February 2005, a car filled with explosives drove into a crowd of military and police recruits in the town of Hillah, Iraq.²⁴ More than one hundred twenty-five people died—the largest death toll for a single incident in Iraq until that time. The suicide bomber's hand and forearm were found chained to the steering wheel of the exploded car (why they were chained is a fascinating question of psychology). When the fingerprints were taken by U.S.

¹⁹ A summary of the al-Banna case can be found in Stewart A. Baker & Nathan A. Sales, "Homeland Security, Information Policy, and the Transatlantic Alliance," in George Mason University Law and Economics Research Paper Series 09-20 (March 2009), <http://ssrn.com/abstract=1361943>. See also Charlotte Buchen, *The Man Turned Away*, PBS FRONTLINE, Oct. 10, 2006, www.pbs.org/wgbh/pages/frontline/enemywithinh/realty/al-banna.html.

²⁰ For a more thorough description of the ATS, see Paul Rosenzweig, "Targeting Terrorists: The Counterrevolution," 34 Wm. Mitchell L. Rev. 5083, 5086–90 (2008). See also Privacy Act of 1974, Notice of Privacy Act System of Records, 72 Fed. Reg. 43,650–02 (Aug. 6, 2007) (providing details of the ATS).

²¹ See Customs and Border Protection, On a Typical Day in Fiscal Year 2009, CBP . . . , http://www.cbp.gov/xp/cgov/about/accomplish/fy09_typical_day.xml.

²² See Scott Shane & Lowell Bergman, "Contained? Adding Up the Ounces of Prevention," *The New York Times*, Sep. 10, 2006, § 4, at 1.

²³ U.S. Customs and Border Protection, CBP: Securing America's Borders 4 (Sept. 2006), http://www.customs.gov/linkhandler/cgov/newsroom/publications/mission/cbp_securing_borders.ctt/cbp_securing_borders.pdf.

²⁴ See Shane & Bergman, *supra*.

military forces, a match was found to the fingerprints taken from al-Banna twenty months earlier in Chicago.

Now, of course, nobody knows what al-Banna intended to do that day when he arrived at O'Hare. It is impossible to prove a counterfactual. Perhaps he was only headed to visit friends, but the CBP officer who interviewed al-Banna later said, "I was shocked. That it was so close to home, that I actually interviewed someone who not only was capable of doing but actually did something like that. You never know who you are interviewing or what they are capable of doing."²⁵ Without the data analysis provided by ATS, it is nearly certain that al-Banna would have entered the U.S.—who knows for what purpose.

Most similar successes are not made public. Often the factors that form part of the analysis cannot be revealed, and successes in identifying terrorist suspects—or, in other contexts, members of a criminal organization—would be negated by disclosure of the success. Only al-Banna's death made his case fit for public disclosure.

That does not mean that a careful observer cannot discern the outlines of other cyber intelligence successes based on data analysis in recent events. When David Headley was arrested for allegedly seeking to commit terrorist acts in Denmark, news reports suggested that one of the key factors in his identification was his pattern of travel to the Middle East and his efforts to conceal those trips from the government.²⁶ Dataveillance of his travel provided both the trigger to ask questions and the factual cross-check on the veracity of his answers. Likewise, when Najibullah Zazi (who tried to explode a bomb in Times Square) was arrested, one factor that was publicly disclosed as a ground for suspicion was his travel to Pakistan.²⁷

Both of these incidents, which involved serious threats of violence, would appear to have been thwarted, at least in part, through some form of successful dataveillance, i.e., using knowledge discovery techniques to target investigative resources based upon a careful risk assessment of seemingly innocent individuated facts.

Our failures also seem to arise when these sorts of cyber analytic techniques are used ineffectively. In the case of the 2009 Christmas bomb plot, not only was Abdulmutallab's name provided by his father, but the evidence suggests that other, less specific NSA intercepts existed that might have generated a suspicion of Nigerian travelers.²⁸ Add in his reported purchase of a ticket with cash and the alleged

²⁵ DHS Success Stories Case # 000016 (2005/03/01) (on file with author).

²⁶ See Cam Simpson & Siobhan Gorman, "Terror Suspect Failed a Test," *Wall St. Journal*, Dec. 9, 2009, at A4.

²⁷ For example, the Department of Justice's Motion for a Permanent Order of Detention cites CBP records of trips to Pakistan. Memorandum of Law in Support of the Government's Motion for a Permanent Order of Detention at 3–4, *United States v. Najibullah Zazi*, No. 09-CR-663 (RJD) (E.D.N.Y. Sept. 24, 2009), <http://www.justice.gov/opa/documents/zazi-detention-memo.pdf>.

²⁸ Umar Farouk Abdulmutallab,

http://topics.nytimes.com/top/reference/timestopics/people/a/umar_farouk_abdulmutallab/index.html.

rejection of his visa application by the U.K.²⁹ and the case seems to be the precise sort of concatenation of facts which, individually, amount to little but, collectively, paint a more cautionary picture. In the wake of the failed bombing attempt, there are already calls for even greater efforts to “connect the dots” of terrorist threats and that will mean more dataveillance, not less.³⁰

Antique Privacy

Cyber dataveillance is here to stay whether we like it or not. The only question is when and how we monitor and control the government’s use of the techniques so that we get the benefits of the growth in data surveillance without the potential harms to civil liberties.

As should be evident, the use of such analytical tools is not without risks. The same systems that sift layers of data to identify concealed terrorist links are just as capable, if set to the task, of stripping anonymity from many other forms of conduct—personal purchases, politics, and peccadilloes. The question then becomes how do we empower data analysis for good purposes while providing oversight mechanisms for deterring malfeasant uses?

Our current privacy-protective architecture, or, if one prefers, our anonymity-protective architecture, is simply not up to the task. It is, to a very real degree, an antique relic of the last century. The relevant Supreme Court precedents date from the 1970s, as does the 1974 Privacy Act.³¹ Is it any wonder that the current structure of law does not match the technological reality?

The “third party doctrine” developed by the Supreme Court in two 1970-era cases—*United States v. Miller*³² and *Smith v. Maryland*³³—at the dawn of the computer era, means that information you disclose to a third party is not protected by the Fourth Amendment. In the context of data privacy, that means that there is no constitutional protection against the collection and aggregation of your cyber data (credit card purchase and the like) for purposes of data analysis and piercing the veil of anonymity.³⁴

²⁹ *Id.*; John F. Burns, “Britain Says Bomb Suspect Was Denied Visa Renewal,” *The New York Times*, Dec. 29, 2009, at A12.

³⁰ See Ben Feller, “Obama: The Buck Stops with Me,” *Huffington Post*, Jan. 7, 2010, http://www.huffingtonpost.com/2010/01/07/obama-christmas-bomber-report_n_414309.html.

³¹ 5 U.S.C. § 552a (2006).

³² 425 U.S. 435 (1976).

³³ 442 U.S. 735 (1979).

³⁴ I should note here an important qualification. In January 2012, the Supreme Court decided *United States v. Jones*, ___ U.S. ___ (No. 10-1259, Jan. 23, 2012), <http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf>. The two concurring opinions in the case suggest that at some future point the Court may revisit the third-party doctrine. For now, however, as Congress considers its legislative options, the existing legal architecture remains unchanged and I take it as settled ... until, of course, it no longer is.

At the federal level, what protects anonymity are the statutory protections created by Congress.³⁵ Some laws, like the Right to Financial Privacy Act (RFPA),³⁶ create sector-specific privacy protections. Reacting to *Miller*, the RFPA prevents banks from willy-nilly providing financial data to the government, instead requiring the issuance of a subpoena and notice to a customer who has the right to object to the inquiry. Likewise, the Health Insurance Portability and Accountability Act³⁷ has stringent rules regarding medical privacy and limiting the types of disclosures that doctors, hospitals, and insurers can make.

By and large, however, in the national security dataveillance sphere there is no sector or activity-specific set of protections.³⁸ Rather, we seek to protect privacy (or anonymity) by requiring the government to adhere to broad principles of privacy protection. These principles, known as the Fair Information Principles,³⁹ were first developed in the U.S. and have now become the touchstone of most privacy protective regimes. They are embedded in the Privacy Act of 1974 and lie at the core of the European Union's 1995 Privacy Directive.⁴⁰ In brief summary—which does not do them justice for want of detail—the principles are:

- *Collection limitation*: The collection of personal information should be lawful and limited to that which is necessary. Where feasible, the collection should be consensual.
- *Data quality*: Those collecting information should strive to ensure that it is accurate, relevant, and complete.
- *Purpose specification*: Data should be collected for a specific purpose. Data should not be repurposed to other uses without disclosure and consent, if at all.
- *Use limitation*: Data should be used only for a specific purpose and should be disclosed only for the purpose collected.
- *Security safeguards*: Information collected should be protected against loss or theft.
- *Openness*: The collection, use, and security of data collected should be fully disclosed and transparent to the public.
- *Individual participation*: Individuals should be allowed to access data collected about themselves and should be afforded a chance to correct any errors they perceive.
- *Accountability*: Those who collect and hold data should be accountable for their adherence to these norms.⁴¹

³⁵ There exist state-based statutory privacy protections and most state courts recognize a common law right to privacy of some form. See Samuel Warren & Louis D. Brandeis, "The Right to Privacy," 4 Harv. L. Rev. 193 (1890). Neither is an effective limitation on the action of the federal government.

³⁶ 12 U.S.C. §§ 3401–3422 (2006).

³⁷ Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 26, 29, and 42 U.S.C.).

³⁸ The Foreign Intelligence Surveillance Act is a notable exception, governing the collection of the substance (as opposed to the call record data) of personal communications. See Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801–1871 (2006).

³⁹ See Privacy Rights Clearinghouse, "A Review of the Fair Information Principles: The Foundation of Privacy Public Policy," <http://www.privacyrights.org/ar/fairinfo.htm>.

⁴⁰ See Privacy Act, 5 U.S.C. § 552a (2006); Council Directive 95/46/EC, 1995 O.J. (L281) 31, http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

⁴¹ See Fair Information Principles, *supra*.

In the U.S., these principles are procedurally implemented through Privacy Impact Assessments (PIAs) and through the publication of System of Record Notices (SORNs).⁴² The PIA, conducted by the government, is a detailed analysis of how a particular set of personal information is collected, stored, protected, shared, and managed. The SORN is the public notification of the existence of systems that collect and hold data. Taken together, the two requirements are intended to provide for the openness and accountability that will allow the public to remain assured that those collecting data are adhering to these principles.⁴³

The problem is that a conscientious and fair application of these principles is, in many ways, fundamentally inconsistent with the way in which personal information can be used in the context of counter-terrorism or cyber insurgency dataveillance. Recognizing this fact is not, at this juncture, to make a normative judgment, but merely to make the descriptive point that the way in which dataveillance programs, like the Automated Targeting System that discovered al-Banna, function is at odds with these principles.

Consider that the collection limitation principle calls for the collection of the least amount of information and, where feasible, acquiring the consent of those about whom the data is being collected. Effective terrorism dataveillance, however, relies on the breadth of the collection for its success since the unknown connection will often come from an unexpected data field and the collection often occurs without the knowledge of, much less the consent of, the data subject.

Likewise, the purpose specification principle, if fully applied, would significantly degrade the analytical utility of many knowledge discovery systems. Often the data of interest that gives rise to a previously unknown connection is one that was collected for a different purpose and intended for a different use. To take the most prosaic example, imagine that a phone number is collected from an air traveler so that the airline may contact him, and his frequent flyer number is collected so that his loyalty account may be credited. When those data fields are used for another purpose—for example, to identify potential connections between known terrorists and those who are otherwise unknown—these purpose and use limitation principles are violated. Yet that is precisely how systems like ATS operate and, in retrospect, it is a method that might have identified the 9/11 terrorists before their attack if it had been available at the time.⁴⁴

⁴² See U.S. Securities and Exchange Commission, *Privacy Impact Assessment (PIA) Guide 4* (Jan. 2007), www.sec.gov/about/privacy/piaguide.pdf.

⁴³ Separately, the Privacy Act also affords individuals the right to go to court to correct erroneous data collected about them. 5 U.S.C. § 552a(d) (2006). It is a never-ending source of friction with our international partners that this right extends only to American citizens and legal residents.

⁴⁴ See Newton N. Minow, "Seven Clicks Away," *Wall St. Journal*, June 3, 2004, at A14; The Markle Foundation, *Protecting America's Freedom in the Information Age: A Report of the Markle Foundation Task Force 28* (2002), http://www.markle.org/downloadable_assets/nstf_full.pdf.

Perhaps even more pointedly, the principles of openness and individual participation are challenging to implement in the counter-terror context. Full disclosure of the methods of operation of a dataveillance system would often make it easier, for those wishing to do so, to evade it. The notion of allowing potential terrorists to see exactly what data is and is not held about them simply seems impossible to contemplate.

The problem, of course, is that in this modern world of widely distributed networks with massive data storage capacity and computational capacity, so much analysis becomes possible that the old principles no longer fit. We could, of course, apply them, but only at the cost of completely disabling the new analytic capacity. In the current time of cyber threat that seems unlikely. Alternatively, we can abandon privacy altogether, allowing technology to run rampant with no control. That, too, seems unlikely and unwise.

What is needed, then, is a modernized conception of privacy—one with the flexibility to allow effective government action but with the surety necessary to protect against government abuse.

Modernizing Privacy

Our privacy laws and our conceptions of privacy cannot withstand the technological change that is happening and the cyber conflict that is developing. We must put theories of data availability and anonymity on a sounder footing—a footing that will withstand the rigors of ever-increasing computational capacity. To do so we need to define what values underlie our instinctive privacy-protective reaction to the new technology, assess how realistic threats of abuse and misuse are, and create legal and policy incentives to foster positive applications while restraining adverse ones.

Though a comprehensive new anonymity-protective legal structure has yet to be developed, the outline of one can already be discerned. Old ideas of collection and purpose limitations will be forced by technological change to yield to a greater emphasis on use limitations. Even those limitations will need to be modified so that our concern is not with uses that are mere “analyses” but rather with uses that constitute the “imposition of adverse consequences.” The new system will be based on the new answers to three broad questions:

- What is privacy?
- What new structural systems do we need?
- What old rules need to be rethought?

What is Privacy? —Privacy is really a misnomer. What it reflects is a desire for independence of personal activity, a form of autonomy. We protect that privacy in many ways. Sometimes we do so through secrecy which effectively obscures both observation of conduct and the identity of those engaging in the conduct. In other instances we protect the autonomy directly. Even though conduct is observed and the

actor identified, we provide direct rules to limit action—as, for example, in the criminal context where we have an exclusionary rule to limit the use of illegally collected evidence.

The concept of privacy that most applies to the new information technology regime is the idea of anonymity or “practical obscurity,” a middle ground where observation is permitted—that is, we expose our actions in public—but we are not subject to identification or scrutiny. The information data-space is suffused with information of this middle-ground sort, e.g., bank account transactions, phone records, airplane reservations, and Smartcard travel logs to name but a few. They constitute the core of transactions and electronic signature or verification information available in cyberspace. The anonymity that one has in respect of these transactions is not terribly different from “real-world anonymity.” Consider, as an example, the act of driving a car. It is done in public, but one is generally not subject to routine identification and scrutiny.

Protecting the anonymity we value requires, in the first instance, defining it accurately. One might posit that anonymity is, in effect, the ability to walk through the world unexamined. That is, however, not strictly accurate, for our conduct is examined numerous times every day. Sometimes the examination is by a private individual—for example, one may notice that the individual sitting next to them on the train is wearing a wedding ring. Other routine examinations are by governmental authorities—the policeman in the car who watches the street or the security camera at the bank or airport, for example. As we drive down the road, any number of people might observe us.

So what we really must mean by anonymity is not a pure form of privacy akin to secrecy. Rather, what we mean is that even though one’s conduct is examined, routinely and regularly, both with and without one’s knowledge, *nothing adverse should happen to you without good cause*. In other words, the veil of anonymity—previously protected by our “practical obscurity”—that is now so readily pierced by technology must be protected by rules that limit when the piercing may happen as a means of protecting privacy and preventing governmental abuse. To put it more precisely, the key to this conception of privacy is that privacy’s principal virtue is a *limitation on consequence*. If there are no unjustified consequences—i.e., consequences that are the product of abuse or error or the application of an unwise policy—then, under this vision, there is no effect on a cognizable liberty/privacy interest. In other words, if nobody is there to hear the tree, or identify the actor, it really does not make a sound.

The appeal of this model is that it is, by and large, the model we already have for government/personal interactions in the physical world. The rule is not that the police cannot observe you; it is that they require authorization of some form from some authority in order to be permitted to engage in certain types of interactions, which are identified here as “consequences.” The police normally cannot stop you to question you without “reasonable suspicion,” cannot arrest you without “probable cause,” cannot search your house without “probable cause,” and cannot examine a corporation’s business records about you without a showing of “relevance” to an ongoing investigation. We can and should build structures that map the same rules-based model of authorization linked to consequence as the appropriate model for the world of dataveillance.

Thus, the questions to be asked of any dataveillance program are: What is the consequence of identification? What is the trigger for that consequence? Who decides when the trigger is met? These questions are the ones that really matter, and questions of collection limitation or purpose limitation, for example, are rightly seen as distractions from the main point. The right answers to these questions will vary, of course, depending on the context of the inquiry, but the critical first step is making sure that we are asking the right questions.

What New Structural Systems Do We Need?—Once defined, how do we protect anonymity?⁴⁵ The traditional way is with a system of rules and a system of oversight for compliance with those rules. Here, too, modifications need to be made in light of technological change.

Rules, for example, tend to be static and unchanging and do not account readily for changes in technology. Indeed, the Privacy Act—the central statute intended to protect individual privacy against government intrusion—is emblematic of this problem; the principles of the Privacy Act are ill-suited to most of the new technological methodologies, such as distributed databases. Thus, we have begun to develop new systems and structures.

First, we are changing from a top-down process of command and control rule to one in which the principal means of privacy protection is through institutional oversight. To that end, the Department of Homeland Security was created with a statutorily required Privacy Officer (and another Officer for Civil Rights and Civil Liberties).⁴⁶ The more recent Intelligence Reform and Terrorism Prevention Act,⁴⁷ and the Implementing Recommendations of the 9/11 Commission Act of 2007⁴⁸ go further. For the first time, they created a Civil Liberties Protection Officer within the intelligence community. More generally, intelligence activities are to be overseen by an independent Privacy and Civil Liberties Oversight Board.⁴⁹ Indeed, these institutions serve a novel dual function. They are, in effect, internal watchdogs for privacy concerns. In addition, they naturally serve as a focus for external complaints, requiring them to exercise some of the function of ombudsmen. In either capacity, they are a new structural invention on the American scene—at least, with respect to privacy concerns.

Second, and perhaps most significantly, the very same dataveillance systems that are used to advance our counter-terrorism interests are equally well suited to assure that government officials comply with

⁴⁵ This section is based in part on the essay Paul Rosenzweig, "The Changing Face of Privacy Policy and the New Policy-Technology Interface," *IEEE Intelligent Systems, Trends and Controversies* 84–86 (Sept.–Oct. 2005), www.dartmouth.edu/~humanterrain/papers/intelligent_systems.pdf.

⁴⁶ See Homeland Security Act of 2002, Pub. L. No. 107-296 § 222 (2002).

⁴⁷ See Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638.

⁴⁸ Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 1502, 121 Stat. 266, 424 (codified at 6 U.S.C.A. § 1152(g) (West 2008)).

⁴⁹ The duties of Civil Liberties and Privacy Officer in the Office of the Director of National Intelligence are codified at 50 U.S.C. § 403-3d (2006). The Privacy and Civil Liberties Oversight Board is authorized by section 801 of the Implementing Recommendations of the 9/11 Commission Act of 2007.

the limitations imposed on them in respect of individual privacy. Put another way, the dataveillance systems are uniquely well equipped to watch the watchers, and the first people who should lose their privacy are the officials who might wrongfully invade the privacy of others.

Indeed, there are already indications that these strong audit mechanisms are effective. Recall the incident in the last presidential campaign in which contractors hacked Barack Obama's passport file.⁵⁰ In this instance, there was no lawful reason for the disclosure of the file; it was disclosed purely for prurient, political reasons. As a result, candidate Obama suffered an adverse consequence of disclosure which had not met any legal trigger that would have permitted the disclosure. A strong audit function quickly identified the wrongdoers and allowed punitive action to be taken.⁵¹

We can, therefore, be reasonably confident that as we move forward in establishing a consequence-based system of privacy protection we are also moving toward a point where the legal structures and technological capabilities to support that system are being put into place.

What Old Rules Need to Be Rethought?—Perhaps the greatest dangers, however, lie in questions that we have yet to ask—at least those that have not yet been heard.⁵² These are questions about the nature of wrongs and the nature of punishment. While these new dataveillance technologies mean greater success in identifying, solving, and punishing wrongful conduct, such as terrorism, they are equally capable of identifying, solving, and punishing wrongful conduct of a more morally ambiguous nature. Consider, as an almost trivial example, the use of red light cameras in several major American cities. Before the development of this technology, drivers running red lights were identified only infrequently when they had the bad luck to run the light in the presence of a police officer. Now, with automated cameras, the rate of capturing wrongful red light runs is higher.⁵³ The same is increasingly true of a host of other offenses. Given the rate and scope of technological development, the trend will only continue. This change—the use of technology to make it more likely (if not certain) that violations of law will be observed—will work powerful effects on the deterrence component of law enforcement and, if properly applied, on criminal and espionage-type activity in cyberspace. We now calculate the optimal level of punishment by discounting the “real” punishment to account for the likelihood of getting caught. A ten-year sentence with a one-in-ten chance of capture arguably has an effective deterrent value of one year in prison. When the chance of capture increases, the effective deterrent does as well.

⁵⁰ See Helene Cooper, “Passport Files Of 3 Hopefuls Are Pried Into,” *The New York Times*, Mar. 22, 2008, at A1.

⁵¹ Two contract employees were fired by the State Department in the Obama case and a third was disciplined. *Id.* In the case of Joe Wurzelbacher (“Joe the Plumber”), whose tax records were disclosed, several Ohio state employees were identified and disciplined. See “Clerk Charged with Unlawful Search of Joe the Plumber,” <http://www.toledoonthemove.com/news/story.aspx?id=213580>.

⁵² I first discussed the ideas in this section with my friend and colleague Kim Taipale of the Center for Advanced Studies. See also K.A. Taipale, *Play Room in the National Security State* (unpublished manuscript, on file with the author) (Center for Advanced Studies Working Paper Series No. 05:0515) (technological changes are transforming criminal justice system from one based on punishment and deterrence to one based on ubiquitous preventative surveillance and control through system constraints).

⁵³ See, e.g., Kevin Courtney, “Red Light Cameras Work, But Are Fines Too High?,” *Napa Valley Register*, Feb. 14, 2010, http://www.napavalleyregister.com/news/local/article_1fbc2456-1932-11df-b32f-001cc4c03286.html.

An interesting corollary to the development of new technologies is that they will, inevitably, require either a reduction in punishments across the board or a much better, and narrower, definition of “wrongful conduct.” As technology trends towards near perfect enforcement, society will need to re-examine its definition of what constitutes a “wrong.” To put it prosaically, in a world where we could identify every Senator who has illegally smoked a Cuban cigar or every individual who has exceeded the speed limit by the least amount, we might well need to change our definition of those acts as wrongful. Increasingly, we will need to consider how we can best enhance individual autonomy, and that may necessitate decreasing the sphere of governmental authority.

Thus, one of the unseen perils to dataveillance is not, as most privacy advocates suppose, the increased likelihood that the state will abuse its power by targeting for adverse consequence those who have committed no crime—for example, a person whose only act is to engage in political protest. The new structures and systems we are putting in place are likely to be capable of protecting against abuse. The real peril is that our conception of the state’s ambit has grown so broad that the state may soon lawfully use its powers to target “wrongful” conduct that ought not, truly, to be deemed wrongful.

Conclusion

It will be a significant challenge to determine the right answers to many of the substantive questions I have posed. There will be substantial policy issues to resolve, for example, in determining what, if any, triggers might be created for denying an individual employment in a nuclear facility or refusing to let him board a plane. Yet these are the questions that must be answered. The improvements in computational power and data storage costs will not slow down, and we cannot expect to stop the deployment of new anonymity-invasive technology. Indeed, any effort to do so is doomed to failure before it has begun.

Therefore, rather than vainly trying to stop progress, or trying to fit the new technologies into old principles of privacy that no longer apply, we will need to go about the business of answering the hard policy questions. Instead of reflexively opposing technological change, a wiser strategy is to accept the change and work within it to channel change in beneficial ways.

This will require a rethinking of privacy—both a re-conception of what we think it means and a reconfiguration of how we think it is to be protected. It may be true that “privacy is dead,” but for those who truly want to protect privacy, the motto should be: “Privacy is dead. Long live the new privacy.”

**Post-Hearing Questions for the Record
Submitted to Ms. Mary Ellen Callahan
Chief Privacy Officer, U.S. Department of Homeland Security
From Senator Ron Johnson**

1. Given your role as the Chief Privacy Officer at DHS and serving as Co-chair of the Privacy Committee of the Federal Chief Information Officers Council, which agencies, in your opinion, have the most robust privacy policies in place? Which agencies need the most improvement?

The former Chief Privacy Officer, Mary Ellen Callahan, left the Department of Homeland Security (DHS) to return to the private practice of law. Deputy Chief Privacy Officer Jonathan Cantor is currently serving as the Acting Chief Privacy Officer until Ms. Callahan's replacement is appointed. The Department is pleased to address your question about robust privacy policies below.

As Ms. Callahan stated in her oral testimony, the DHS Chief Privacy Officer has strong statutory authorities and oversees an office that is appropriately resourced to carry out those functions. These two elements have enabled DHS to build a core professional privacy staff and develop robust Departmental privacy policies, many of which are regarded as models throughout the federal government. DHS works with component offices from the outset to integrate privacy protections into new programs, systems, and initiatives. In addition, the Department follows up with components to review compliance with Privacy Impact Assessments through Privacy Compliance Reviews and other oversight mechanisms.

Though the achievements of DHS and the federal privacy community at large are substantial, areas for improvement remain. Like DHS, agencies within the Federal Chief Information Officers Council have expressed their ongoing desire to improve and perfect existing privacy policies. Many agencies encounter difficulty upgrading old databases or migrating information to new storage solutions, such as cloud computing. Social media is one area that requires further study by federal agencies in terms of existing approaches to privacy. The Department acknowledges the complexity of these issues, which is one reason why participation in the Privacy Committee of the Chief Information Officers Council is so vital. As discussed in Ms. Callahan's testimony, the Privacy Committee shares best practices among federal privacy professionals to ensure that we can collectively improve the privacy practices of all federal agencies and address new challenges in a consistent and efficient manner.

2. Is the privacy committee discussing retention periods within agencies for information that is no longer needed?

Within agencies, are there processes for deleting information?

The Privacy Committee of the Chief Information Officers Council discusses many of the issues of interest to the federal privacy community, including data retention periods. These conversations take place within the context of a given privacy matter, such as reducing the risk of a privacy incident. Much of the specific, detail-oriented discussion of data retention policy, however, takes place at the agency level. At DHS, the Privacy Office works with component offices to evaluate data retention periods and to identify the nexus between the data retention period and the impact on the office's mission. The Department reviews record retention schedules as part of the Privacy Impact Assessment and System of Records Notice process and conducts routine reviews to ensure that record retention schedules are appropriate to the data collected and approved by the National Archives and Records Administration (NARA). The Department has also issued a DHS directive to satisfy the requirements of Office of Management and Budget (OMB) Memoranda 06-16 and 07-16, regarding the appropriate handling and maintenance of computer-readable extracts.

Retention periods remain a topic of ongoing discussion within the Department, and one that we consider in consultation with NARA to ensure that DHS complies with applicable records schedules.

3. Can you elaborate on how many different rules, regulations, laws in the Federal Government run counter to each other when it comes to privacy policy?

One of the more significant challenges in applying federal privacy rules, regulations, and laws is that some of those authorities were created in the context of a specific technological paradigm, and thus may be challenging to apply as technology advances. Some statutes or regulations are more stringent or specific than others; typically, however, the federal privacy authorities complement each other as reinforcing layers that provide effective safeguards. DHS, for example, has implemented regulations under the Privacy Act of 1974 that provide additional detail that is specific to DHS. The specificity of DHS' regulations does not, however, run counter to the Department's statutory obligations under the Privacy Act. Rather, the regulations complement and further specify the Department's statutory requirements and procedures. On the whole, the existing landscape of federal laws and regulations forms a fabric of privacy protection that has helped DHS and other agencies embed privacy throughout federal programs and systems.

**Post-Hearing Questions for the Record
Submitted to Mr. Greg Long
Executive Director, Federal Retirement Thrift Investment Board
From Senator Daniel Akaka**

**“State of Federal Privacy and Data Security Law: Lagging Behind the Times?”
July 31, 2012**

1. In 1999, the Office of Management and Budget directed agencies to identify a senior agency official responsible for information privacy issues. In 2008, the Government Accountability Office examined 12 large agencies and found that several of the senior privacy officials did not have oversight of all key privacy functions.
 - a. Please discuss the duties and authorities of the Federal Retirement Thrift Investment Board’s (Board) designated privacy official.

The General Counsel of the FRTIB serves as the agency’s designated privacy official. The General Counsel is responsible for overseeing the FRTIB’s compliance with all applicable privacy requirements of the Privacy Act and the E-Government Act of 2002, as well as any other privacy initiatives that are deemed in the best interest of the Thrift Savings Plan’s participants and beneficiaries. The General Counsel’s responsibilities also include ensuring that the FRTIB’s Systems of Record Notices and Privacy Act notices are up-to date, that the FRTIB performs Privacy Threshold Analyses and any required Privacy Impact Assessments, and that appropriate FRTIB staff and contractor staff are trained regarding privacy considerations.

- b. Please discuss how the Board ensures that the designated privacy official is able to adequately oversee all key privacy functions.

The Board has established a Privacy Act initiative, led by the General Counsel as the Agency’s designated privacy official. In addition to representatives from the Office of General Counsel, the team is staffed with representatives from other offices involved in overseeing Agency records systems, including the information security office, the benefits office, the risk management office and the records office. This team will develop procedures for ensuring Privacy compliance throughout the Agency and its contracting staff. As part of this effort, the General Counsel will be hiring a new staff member to handle day-to-day Privacy Act functions, as well as a senior attorney who will be tasked with the oversight of Privacy Act compliance. Based upon the recommendations of the Privacy Act Team, additional steps and resources may be required.

- c. Please explain the circumstances, timing, and rationale for the recent transfer of privacy responsibilities from the Director of Administration to the General Counsel.

In the 2003-2004 timeframe, a decision was made by the prior Executive Director to reduce the size of the Federal employees working for the FRTIB. As a result, the number of employees actually on board went from slightly less than 100 to the mid-60s. As a result, the number of employees in the Office of Administration shrunk. During that period, the duties of the designated privacy official were shifted to the Office of General Counsel which has performed them since the transfer. While that transfer was not documented at the time, the current

Executive Director formally designated the General Counsel as the Board's designated privacy official on August 2, 2012.

2. The Board's May 25, 2012, breach notification letter alerted affected individuals that they are eligible for free credit monitoring. However, only approximately 16,000 people – or 13 percent – of those impacted have signed up.
 - a. What additional outreach, if any, has the Board made to encourage people to monitor their credit?

The FRTIB has not made additional outreach. There was wide coverage of the cyber attack in media, particularly media read by Federal employees and the uniformed services, and we believe people were adequately informed. To date, 20,934 affected individuals, or 17 percent, have enrolled in the credit monitoring, which exceeds industry standards of roughly 10 percent.

- b. Please explain whether the Board initiated or is planning to initiate any other follow-up assistance to those impacted by the data breach?

Please see answer to question 2a above.

**Post-Hearing Questions for the Record
Submitted to the Mr. Greg Long
Executive Director, Federal Retirement Thrift Investment Board
From Senator Tom Carper**

**“State of Federal Privacy and Data Security Law: Lagging Behind the Times?”
July 31, 2012**

1. Many Americans were very troubled to learn about the data breach at the Thrift Savings Plan. While the breach occurred at one of your contractor sites, it still raises questions about your agency’s cybersecurity efforts and your oversight of contractors. Audits produced by the Department of Labor and the Government Accountability Office highlight a number of cybersecurity gaps at the Federal Retirement Thrift Investment Board going back several years. Given the security vulnerabilities identified by the Department of Labor and others, why didn’t the Federal Retirement Thrift Investment Board take more action to address the concerns raised in the audits? If the lack of resources was part of the reason, please explain any fiscal, operational, or administrative changes the Board is making or contemplating to remedy previous funding shortfalls in order to better meet its future IT security needs.

The past decade has been a time of dramatic expansion for the agency, in the number of participants, the dollars invested in the TSP, and the services provided to our participants and beneficiaries. This growth taxed the agency’s ability to complete all that needed to be done.

While we have open IT and security audit recommendations from the Department of Labor, we have been keenly focused on upgrading our infrastructure and security across the past ten years. We have created new call centers, instituted a back up data center to ensure continuity of operations, updated our record keeping software, purchased a new mainframe, developed disaster recovery plans and testing for those recovery plans, mainframe, modernized the TSP network (including providing for full redundancy and high availability), initiated a virtual infrastructure, deployed a new www.tsp.gov website, and implemented test tools. These efforts speak to major IT or IT support activities that provided technical controls to improve our IT security posture, especially with respect to technical controls.

On September 24, 2012, I will present the Board with my budget request for FY2013. That budget will contain an increase in funds and staffing that will allow the FRTIB to make significant progress in addressing the open audit recommendations.

2. In your testimony, you outlined several steps you are now taking to enhance IT security for the Thrift Savings Plan. Please discuss how these enhancements meet the agency’s obligations under the Federal Information Security Management Act. Please also describe any outstanding audit recommendation from the Department of Labor and your timeline for closing the recommendations.

The Agency is in the process of responding to a number of IT Security audit recommendations. Actions that we have taken in the past several months are responsive to the audit

recommendations and we plan to address several additional recommendations by the end of the year. We anticipate that the Department of Labor will be reviewing the status of these recommendations during their FY2013 IT security audits.

The audit recommendations can be classified in the following categories: governance of information systems, such as systems lifecycle, information security, and privacy.

Systems lifecycle: To address these findings, the Agency has implemented several significant efforts to improve its management of information systems:

- A Software Development Lifecycle policy for addressing software development management; and is working on a System Development Lifecycle approach to complement the Software methodology;
- A security lifecycle methodology (as part of the Enterprise Information System Risk Management program), which will be integrated with the Systems and Software Development Lifecycle methodologies;
- A project management framework, which was used on several recent major projects, including the implementation of the Roth feature; and
- A Request for Proposal (RFP) for our record keeping contractor will be issued by the end of December 2012, which will include performance and security requirements. The new contract is expected to be awarded by the end of FY2013.

Information Security: A key milestone in resolving these findings occurred in September of 2011 when I approved an Agency Directive establishing the Enterprise Information System Risk Management (EISRM) program that provides a framework for the Agency to manage risk associated with information systems. On June 29, 2012, I approved eighteen constituent control family policies, derived from NIST Special Publication 800-53rev3, which establish the requirements of the program. We are now moving to implement the processes that will ensure compliance with these policies.

Privacy: The EISRM addresses the proper security categorization of information and information systems and the proper handling of PII. The Agency issued a breach notification plan in June of 2012. The Agency has a team in place to focus on conducting Privacy Impact Assessments (PIAs).

3. What near and long-term steps are you taking to improve the IT security requirements in your contracts and to strengthen your oversight of the contractors that manage the Thrift Savings Plan?

The FRTIB is enhancing the IT security clauses in its contracts, as the contracts come up for re-bid or renewal. We are adding more detail regarding data breach requirements, as well provisions relating to security audits, personnel security (screening and rescreening), security and privacy training requirements, and integration of specific FISMA and Privacy Act requirements.

The RFP for the recordkeeping contract will incorporate many of these additional clauses as well as several others which integrate specific FRTIB security requirements as established by the Agency's EISRM program's requirements which are derived in large part from FISMA. We have retained Gartner Consulting to assist us in the development of this RFP to ensure we are incorporating industry best practices into the contract on all fronts.

**Post-Hearing Questions for the Record
Submitted to Mr. Greg Long
Executive Director, Federal Retirement Thrift Investment Board
From Senator Ron Johnson**

**“State of Federal Privacy and Data Security Law: Lagging Behind the Times?”
July 31, 2012**

1. Can you please explain DHS’ role in assisting FRTIB with IT security policies and practices? What third-party providers do you rely on for IT security?

As required by FISMA, the FRTIB notified US-CERT within one hour of determining that personally identifiable information had been accessed as a result of the cyber attack. US-CERT requested information, which we provided as it became available. During the incident response and breach notification process, we did not receive assistance from DHS.

We subsequently became aware that DHS was offering “Red Team”/“Blue Team” assistance to agencies. We have spoken with DHS in a very preliminary manner to determine what services DHS could provide to the FRTIB and will keep that resource in mind as we move forward with our Tiger Team review.

Operationally, we receive third-party IT security support from Serco and its subcontractors. Additionally, we have contracted with an independent company to provide consulting and program support assistance to the CISO and the Tiger Team. We will propose a budget request to continue and increase that independent support in FY13.



August 24, 2012

The Honorable Daniel Akaka
 Chairman
 Subcommittee on Oversight of Government Management, the Federal Workforce, and
 the District of Columbia
 Committee on Homeland Security and Governmental Affairs
 United States Senate

Subject: *GAO Response to a Post-Hearing Question on Agency Retention Policies*

Dear Mr. Chairman:

It was a pleasure to appear before your Subcommittee on July 31, 2012 to discuss updating federal privacy law to address a changing technology landscape.¹ This letter responds to a request that I provide an answer to a post-hearing question from Senator Johnson for the record. The question, along with my response, follows.

1. You testified about the need of limiting the data the Federal Government obtains and then the amount of time it is retained. Which agencies currently have retention policies in place?

Each federal agency is to have data retention policies in place. According to the Federal Records Act² each agency is required to make and preserve records that (1) document the organization, functions, policies, decisions, procedures, and essential transactions of the agency and (2) provide the information necessary to protect the legal and financial rights of the government and of persons directly affected by the agency's activities.³

To do this, agencies are to develop record retention schedules with the assistance and approval of the National Archives and Records Administration (NARA)⁴ or use general schedules developed by NARA. These schedules identify federal records and timeframes for their destruction or archiving.

¹GAO, *Privacy: Federal Law Should Be Updated to Address Changing Technology Landscape*, GAO-12-961T (Washington, D.C.: July 31, 2012).

²44 U.S.C. chapters 21, 29, 31, and 33.

³44 U.S.C. § 3101.

⁴NARA is responsible for issuing records management guidance for adhering to the Federal Records Act; working with agencies to implement effective controls over the creation, maintenance, and use of records in the conduct of agency business; providing oversight of agencies' records management programs; approving the disposition (destruction or preservation) of records; and providing storage facilities for agency records.

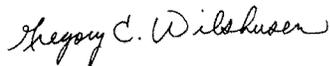
GAO has not done a comprehensive review of the federal records scheduling and disposition process, and so we do not have information specifically about which agencies have records retention policies in place.

However, NARA has released a yearly report⁵ on its records management self-assessment, which analyzes responses to a survey sent to over 220 federal cabinet-level agencies, agency components, and independent agencies. NARA's 2009 survey⁶ indicated, among other things, that a large proportion of agencies had not scheduled existing systems that contain electronic records. In the 2010⁷ and 2011⁸ surveys, NARA found that the majority of Federal agencies records management programs scored in the high to moderate risk categories, with records disposition, training, compliance monitoring and the management of electronic records continuing to be significant challenges for agencies.

Additionally, OMB has set requirements to limit the time that information is kept on mobile devices and computers. OMB memorandum 06-16 requires all departments and agencies to keep logs of all computer-readable data extracts from databases holding sensitive information, including extracts stored on mobile devices and to verify that each extract, including sensitive data, is erased within 90 days unless its use is still required past that time. GAO has not conducted audit work to determine how well agencies have been complying with this requirement.

In preparing this correspondence, we relied on previously issued GAO products, OMB guidance, and the NARA 2011 Records Management Self-Assessment Report. Should you or your office have any questions on matters discussed in this letter, please contact me at (202) 512-6244, or John de Ferrari, Assistant Director, at (202) 512-6335. We can also be reached by e-mail at wilshuseng@gao.gov and deferrarij@gao.gov, respectively.

Sincerely Yours,



Gregory C. Wilshusen
Director, Information Security Issues

⁵NARA issued its first self-assessment report in 2010.

⁶NARA, *Records Management Self-Assessment 2009: An Assessment of Records Management Programs in the Federal Government* (April 2010); 220 agencies responded, for a response rate of 91 percent.

⁷NARA, *Records Management Self-Assessment 2010: An Assessment of Records Management Programs in the Federal Government* (February 2011); 251 agencies responded, for a response rate of 93 percent.

⁸NARA, *Records Management Self-Assessment 2011: An Assessment of Records Management Programs in the Federal Government* (May 2012); 247 agencies responded, for a response rate of 89 percent.

**Post-Hearing Questions for the Record
Submitted to Mr. Peter Swire
C. William O'Neill Professor of Law, Ohio State University
From Senator Daniel Akaka**

**“State of Federal Privacy and Data Security Law: Lagging Behind the Times?”
July 31, 2012**

1. As evidenced by the recent data breach affecting over 123,000 Thrift Savings Plan participants and the massive data breach at the Department of Veterans Affairs in May 2006 that impacted 26.5 million veterans and active duty members of the military, federal agencies continue to struggle with protecting personal information. What new or changed requirements would be most effective at reducing the proliferation of data breaches at federal agencies?

Swire: I am not aware of any specific provisions that I would recommend for change.

2. The Office of Management and Budget's (OMB) last major guidance for implementing the Privacy Act was issued in 1975. Given the advances in technology and the new ways in which information is accessed and shared, do you believe an update of OMB's guidance would be useful, and if so, what recommendations do you have for how it should be updated?

Swire: We considered doing such an update when I worked in OMB from 1999 to 2001. My view at the time was that an update would take a great deal of work, likely including extensive public comments to do it well. At the time, I also did not know how best to change the guidance in order to make the overall effects of the Privacy Act significantly better. We therefore focused our limited resources on other projects at that time, including the HIPAA medical privacy rule, the GLBA financial privacy rule, and a project on how to update wiretaps for the Internet age.

In my testimony, I suggested that a more fruitful approach might be to improve the Privacy Impact Assessments under the E-Government Act of 2002.

**Post-Hearing Questions for the Record
Submitted to Mr. Chris Calabrese
Legislative Counsel, American Civil Liberties Union
From Senator Daniel Akaka**

**“State of Federal Privacy and Data Security Law: Lagging Behind the Times?”
July 31, 2012**

1. As evidenced by the recent data breach affecting over 123,000 Thrift Savings Plan participants and the massive data breach at the Department of Veterans Affairs in May 2006 that impacted 26.5 million veterans and active duty members of the military, federal agencies continue to struggle with protecting personal information. What new or changed requirements would be most effective at reducing the proliferation of data breaches at federal agencies?

The first step would be to create a breach notification policy that does not give federal agencies so much latitude regarding when to disclose breaches. Under current OMB policy, agencies may evaluate whether a breach is likely to cause harm and are in some cases actively discouraged from providing such notice (“A number of experts have raised concerns about unnecessary notification and the chilling effect this may have on the public.” OMB Guidance at 15.)

Instead of giving agencies so much latitude, OMB and Congress should embrace the model created by the HITECH Act which governs breaches of medical records. 42 U.S.C. § 17932. The HITECH Act requires covered entities to “notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach.” Unsecured protected health information is defined by the Secretary of HHS. By requiring breach notification anytime unsecured data is lost, agencies have an incentive to embrace data security in order to avoid the public embarrassment of breach notification.

In addition, an agency can do more to reduce the harm caused by breaches by following basic guidelines of the Privacy Act and “maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency”. 5 U.S.C. § 552a (e)(1). If agencies delete sensitive information, such as Social Security numbers and other personal information, once it is no longer needed, they substantially reduce the potential harm from any breach.

In regard to technical standards, defending against hacks and accidental data loss require different technologies. The massive data breach at the Department of Veterans Affairs that involved the loss of personal data about more than 26 million veterans likely could have been avoided through the use of disk encryption software. This technology would protect data in storage such that the data on lost or stolen laptops and backup drives would be inaccessible without the associated encryption password. Federal agencies and government contractors should use disk encryption technology on all computers that store sensitive or other personally identifiable data. It should be pre-installed and enabled by default so that individual employees

are not burdened with configuring it (a task they may neglect to do, and thus put the data of millions at risk).

It is unlikely that the data breach at the Thrift Savings Plan could have been prevented through the use of disk encryption technology, as the data breach involved an attack by hackers, rather than the loss or theft of a laptop. Realistically, protecting systems against hackers is a much more difficult task, and there is no single technology that can provide 100% protection. There is of course quite a bit of low hanging fruit (some of which is routinely ignored by federal agencies), such as promptly installing security updates, and using up to date web browsers. For example, countless security experts have recommended that organizations migrate away from Microsoft's aging Internet Explorer web browser, yet its use in federal government agencies and other large enterprises remains widespread.

Rather than a specific technology, breaches against hackers can best be prevented by regularly bringing in outside security consultants who will attempt to find security holes in the network, unpatched computers, and other flaws. Responsible companies regularly bring in experts to engage in such 'red team' testing - this practice should also be the norm at federal agencies.

**Post-Hearing Questions for the Record
Submitted to Mr. Chris Calabrese
Legislative Counsel, American Civil Liberties Union
From Senator Ron Johnson**

**“State of Federal Privacy and Data Security Law: Lagging Behind the Times?”
July 31, 2012**

1. During the hearing you were asked to give specific examples of purposeful misuse by the government of personal privacy information. Can you please provide these specific examples?

The government collects, stores, and shares a vast amount of American citizens’ personal data. These records include sensitive medical and employment history, contact details like home addresses or phone numbers, financial information, and even detailed location information. Despite rules, audits, and other safeguards meant to protect individuals’ privacy, personal information stored in government databases is frequently accessed and shared improperly. In addition, new technologies have allowed governments to collect information in ways never imagined by our outdated privacy laws, leaving Americans’ rights at risk.

Specific examples of purposeful misuse by the government and government employees of personal privacy information include the following:

- Minnesota’s CityPages.com reported that the DMV record of a former female police officer had been illegally accessed 425 times by 104 officers in 18 different agencies across the state¹. The violations—which took place over several years—led to the woman being stalked, harassed, embarrassed, and ultimately resulted in her having to leave town to try to reclaim her privacy.
- In April an IRS worker admitted to using the agency’s service database to snoop on her ex-husband and others². The technician looked up the contact information of two relatives and a friend, all of whom she had lost touch with.
- The New York Times reported on a story of the Food and Drug Administration (FDA) spying on scientists³. Although the agency claimed to be looking for the unauthorized sharing of trade secrets, the scientists claimed they were being targeted for trying to shed light on an unethical review process. The investigation resulted in a cache of more than 80,000 pages of computer documents, including emails sent privately to members of Congress, lawyers, labor officials, journalists, and even President Obama.

¹ Lussenhop, Jessica. “Is Anne Marie Rasmusson too hot to have a driver’s license?” *CityPages.com*, 22 Feb. 2011

² Pulkkinen, Levi. “IRS Worker Caught Snooping on Ex, Others.” *Seattle PI*, 23 April 2012

³ Shane, Scott. “Vast FDA Effort Tracked E-Mails of Its Scientists.” *The New York Times*, 14 July 2012

- The Washington Post recently reported a story regarding stepped up electronic surveillance of workers across the federal government⁴. One spyware software company, SpectorSoft, claims to have clients in dozens of federal agencies. According to the Post, “It could be programmed to intercept a tweet or Facebook post. It could snap screen shots of their computers. It could even track an employee’s keystrokes, retrieve files from hard drives, or search for keywords.”
- Ars Technica reported on a recent FOIA request by the Electronic Privacy Information Center that found the United States Customs and Border Protection (CBP) agency is sharing data gathered from License Plate Readers (LPR)—including precise GPS location, date, and timestamp information—with an auto insurance umbrella organization called the National Insurance Crime Bureau (NICB)⁵. Every 24 hours, the NICB receives an electronic data transfer from all border stations, providing LPR details on all cars that have crossed in and out of the country. NICB said that, though it is not shared freely with insurance companies and only designated individuals have access, the CPB’s LPR data—“roughly 15 million reads a month”—is kept for 12 months. That means the CBP makes approximately 500,000 LPR reads at the borders every single day, and passes that data along to the NICB. The agreement also allows the NICB to sub-contract management of this data to a “data processing service,” and requires that any misuse of the LPR data be reported to the NICB, and then reported on to the CBP.

While law enforcement needs to collect information, government also needs to recognize that abuse will always be a temptation and take steps to protect our privacy. One key avenue to mitigate these risks is to update our privacy laws to include strict data retention rules so that only what is absolutely necessary is collected and the information is held only as long as necessary.

⁴ Rein, Lisa. “Stepped-up computer monitoring of federal workers worries privacy advocates.” *The Washington Post*. 16 Aug. 2012.

⁵ Farivar, Cyrus. “License plates scanned at border, data shared with car insurance group.” *Ars Technica*. 22 Aug. 2012.

**Post-Hearing Questions for the Record
Submitted to Mr. Paul Rosenzweig
Visiting Fellow, The Heritage Foundation
From Senator Daniel Akaka**

**“State of Federal Privacy and Data Security Law: Lagging Behind the Times?”
July 31, 2012**

1. As evidenced by the recent data breach affecting over 123,000 Thrift Savings Plan participants and the massive data breach at the Department of Veterans Affairs in May 2006 that impacted 26.5 million veterans and active duty members of the military, federal agencies continue to struggle with protecting personal information. What new or changed requirements would be most effective at reducing the proliferation of data breaches at federal agencies?

Data breaches at Federal agencies are no different than data breaches at any large institution. For the most part they are the product of human error and additional requirements or laws would be unnecessary (and, indeed, counter-productive in some cases). The most effective way of reducing data breaches at Federal agencies (which have proliferated at no greater rate than breaches in the private sector) is education and training. Employees need to understand existing policies of usage – changing passwords; not keeping sensitive data on laptops or transportable media; and refraining from clicking on suspicious links, for example – and implement existing protocols.